Comments of

TechFreedom[1]
Berin Szoka, President
Tom Struble, Legal Fellow

International Center for Law and Economics[2]
Geoffrey Manne, Executive Director
Ben Sperry, Associate Director

In the Matter of

Big Data and Consumer Privacy in the Internet Economy

Docket No. 140514424-4424-01

August 5, 2014

[1] Berin Szoka is President of TechFreedom, a nonprofit, nonpartisan technology policy think tank. He can be reached at bszoka@techfreedom.org. Tom Struble is a Legal Fellow at TechFreedom. He can be reached at tstruble@techfreedom.org.

[2] Geoffrey A. Manne is the founder and Executive Director of the nonprofit, nonpartisan International Center for Law and Economics (ICLE), based in Portland, Oregon. He is also Senior Fellow at TechFreedom. He can be reached at gmanne@laweconcenter.org. Ben Sperry is ICLE's Associate Director. He can be reached at bsperry@laweconcenter.org.

If the purpose of this enterprise is for, as the White House's Big Data Report ordered, NTIA to "devise draft legislative text for consideration by stakeholders and submission by the President to Congress,"[3] the agency has simply missed the key questions:

1. What is wrong with U.S. privacy law, whether in substance or process, that needs fixing?
2. How should we go about assessing whether propose legislative reforms would actually be worth adopting?
3. What evidence do we have to inform such assessments?

A serious assessment of the need for new privacy legislation, and the right way to frame it, would not begin by assuming the premise that a particular framework is necessary. Specifically, before recommending any new legislation, the NTIA should do – or ensure that *someone* does – what the Federal Trade Commission has steadfastly refused to do: carefully assess what is and is not already covered by existing U.S. laws.

That inquiry should begin by assessing the extent to which Section 5 of the FTC Act[4] already provides the "comprehensive baseline privacy" protection that has long been the declared goal of those advocating new privacy regulation. After all, it applies to nearly every company in America – and, if anything, we would support extending it to common carriers, too. Of course, the FTC also enforces a variety of other laws, from the Fair Credit Reporting Act to the Children's Online Privacy Protection Act. The FTC, after a supposedly extensive study of the data collected from lading "data brokers" under a Section 6(b) (quasi) subpoena, recently issued a call for legislation to address the problem of data brokers.[5] Exhibit A in their report? The interest categories developed for motorcyclists might also be used to discriminate against them for insurance eligibility.[6] The FTC featured this example prominently in its report and in the press release associated with it[7] – yet made no mention whatsoever of the

[3] Exec. Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, 60 (May 2014) [Big Data Report], *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[4] 15 U.S.C. § 45.
[5] Fed. Trade. Comm'n, *Data Brokers: A Call for Transparency & Accountability* (May 2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[6] *Id.* at vi, 48.
[7] Fed. Trade. Comm'n, *FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information* (May 27, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more.

FTC's previous interpretation of the Fair Credit Reporting Act as applying to precisely such situations: the use of participation in hazardous sports as a characteristic that could influence eligibility determinations, such as for insurance.[8]

Existing laws might well be inadequate to deal with some of the specific the challenges raised by Big Data. But until they are more carefully examined, we will not know where the gaps are. Even those who might insist that there would be no harm to redundancy should agree that we must learn from the lessons of past experience with these laws. Moreover, it is essential to understand what existing law covers because either (a) it will co-exist with any future privacy law, in which case companies will have potentially conflicting

Ideally, such a study should be conducted by the FTC itself as the nation's premiere consumer protection law enforcement agency. But the FTC has stubbornly refused to examine such questions, even to the point of willfully ignoring its own existing authority.

The FTC's Bureau of Consumer Protection (BCP) has issued a flurry of reports on consumer privacy, but has failed to incorporate economic analysis into those reports in any meaningful way – despite having direct access to the top cluster of talented economists inside the Federal government, the FTC's Bureau of Economics (BE). Competition law has been actively shaped by ongoing collaboration between BE and the FTC's Bureau of Competition, but the same cannot be said for consumer protection law, especially around high tech issues such as privacy and data security. On top of this stubborn institutional resistance, it must be noted that the FTC is an independent agency, and therefore directly answerable only to Congress and not the Administration.

For all these reasons, the most useful thing Commerce could do would be to request that Congress immediate create a Privacy Law Modernization Commission modeled on the Antitrust Modernization Commission, which Congress established in 2002 for four purposes:

> (1) to examine whether the need exists to modernize the antitrust laws and to identify and study related issues;

[8] Fed. Trade Comm'n, Bureau of Consumer Prot., *Consumer Reports: What Insurers Need to Know* (Oct. 1998), *available at* http://www.business.ftc.gov/documents/bus07-consumer-reports-what-insurers-need-know ("The FCRA is designed to protect the privacy of consumer report information and to guarantee that the information supplied by credit reporting agencies (CRAs) is as accurate as possible. Consumer reports may include information on an applicant's credit history, medical conditions, driving record, criminal activity, **and hazardous sports**." (emphasis added)).

(2) to solicit views of all parties concerned with the operation of the antitrust laws;

(3) to evaluate the advisability of proposals and current arrangements with respect to any issues so identified; and

(4) to prepare and submit to Congress and the President a report.[9]

A Privacy Law Modernization Commission could do what Commerce on its own cannot, and what the FTC could probably do but has refused to do: carefully study where new legislation is needed and how best to write it. It can also do what no Executive or independent agency can: establish a consensus among a diverse array of experts that can be presented to Congress as, not merely yet another in a series of failed proposals, but one that has a unique degree of analytical rigor behind it and bipartisan endorsement. If any significant reform is ever going to be enacted by Congress, it is most likely to come as the result of such a commission's recommendations.

Attached as appendices are materials by us and others that we believe will assist the Commerce Department's consideration of these issues.

- **Appendix A**: Comments of TechFreedom on Government "Big Data": Request for Information by the Office of Science and Technology Policy (Mar. 31, 2014).[10]
    - Economics, especially studies of how regulation affects innovation in general and small companies in particular, must play a vital role in assessing the trade-offs inherent in any new privacy legislation.
    - So, too, must proposals for new legislation take into account the First Amendment interests at stake.
    - The greatest privacy threats come from government itself, and must be addressed as part of any broad modernization of U.S. privacy laws.
    - Any modernization of U.S. privacy laws must include a careful examination of the FTC's current processes, authority and capabilities, especially insofar as the FTC itself is responsible for administering new privacy laws.

[9] Antitrust Modernization Commission Act of 2002, Pub. L. No. 107-273, §§ 11051-60, 116 Stat. 1856; *see id.* at § 11053.
[10] *Available at* http://docs.techfreedom.org/Comments_Big_Data.pdf.

- **Appendix B**: FTC TECHNOLOGY & REFORM PROJECT, CONSUMER PROTECTION & COMPETITION REGULATION IN A HIGH-TECH WORLD: DISCUSSING THE FUTURE OF THE FEDERAL TRADE COMMISSION (Dec. 2013).[11]
    - This report lays out initial questions to be considered by a working group of FTC scholars and veterans assembled around the FTC's 100th anniversary in considering how to enhance and focus the FTC's efforts, particularly through greater integration of economics into its work and the development of technological capability analogous to the Bureau of Economics' expertise in that field.
- **Appendix C**: *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?: Before the House Energy & Commerce Comm. Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (Mar. 29, 2012) (testimony of Berin Szoka, President, TechFreedom).[12]
    - Transposing abstract principles into actionable legal standards is what really matters.
    - Examines the White House's proposed principles in turn.
    - Considers effective enforcement and the necessary institutional capability.
    - Discussed smart, machine-readable disclosure as a way of empowering consumers while also facilitating easier enforcement.
- **Appendix D**: Responses to Questions for the Record of Berin Szoka, TechFreedom (Mar. 29, 2012).
    - Lays out detailed steps the FTC and Congress could take to enhance U.S. privacy protections.
    - Offers a conceptual framing for how to think about true common law versus the FTC's quasi-common law.
    - Cautions against the mistakes of overly rigid codification, such as the Video Privacy Protection Act.
    - Discusses Do Not Track in particular, reproducing a white paper submitted to the W3C.

[11] *Available at* http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf.

[12] *Available at* http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Szoka-CMT-Balancing-Privacy-and-Innovation-President-Proposal-2012-3-29.pdf.

- **Appendix E**: *The Need for Privacy Protections: Is Industry Self-Regulation Adequate?: Before the Senate Commerce Comm.*, 112th Cong. (Jun. 28, 2012) (testimony of Berin Szoka, President, TechFreedom).[13]
    - Defends American layered approach to privacy protection.
    - Lays out detailed steps the FTC and Congress could take to enhance U.S. privacy protections.
- **Appendix F**: Geoffrey Manne, *Humility, Institutional Constraints and Economic Rigor: Limiting the FTC's Consumer Protection Discretion* (ICLE White Paper No. 2014-1, Jul. 31, 2014).[14]
    - Calls on FTC to better incorporate sound economic- and evidence-based analysis in both its substantive decisions as well as in its process, especially regarding data and privacy.
    - While the FTC has a strong tradition of economics in its antitrust decision-making, its record in using economics in other areas is mixed (or at least opaque). Meanwhile, a review of some recent decisions at the agency suggests that the Commission is inconsistent in its application of economic principles.
    - On privacy (among and other areas), the FTC operates almost entirely by settling enforcement actions in consent decrees. Consent decrees, generally with 20-year terms, are also increasingly becoming a tool for informal policymaking, allowing the Commission to require individual companies to agree to things that are not required by law and thus might more appropriately be addressed on a general basis through the FTC's essentially forgotten Magnuson-Moss rulemaking process.
    - With nearly every major large technology company operating under a consent decree, many have asked whether the FTC is moving towards a form of regulation in which its discretion will be even less constrained, as companies face additional pressure to settle alleged violations of consent decrees because they face monetary penalties (unavailable in Section 5 cases) and even worse public relations fallout than for Section 5 violations.

[13] *Available at* https://docs.google.com/a/techfreedom.org/file/d/0B2pNWHJ8ackuVDVBbFpoTklzOEE/edit.

[14] *Available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474523.

- It is unclear what limits (if any) exist on the FTC's discretion in setting the terms of consent decrees and thus on its ability to make policy via consent decree, such as by requiring "privacy by design" or "security by design."

- **Appendix G**: Comments of TechFreedom on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers: A Preliminary FTC Staff Report of the Bureau of Consumer Protection, Federal Trade Commission, (Feb. 18, 2011).[15]
  - For the FIPPS to be useful, they must be appropriately tailored and relevant for their intended use, -- in other words, adapted to reflect the competing values at stake.
  - They must also allow for ongoing evolution, just as Section 5 has done with deception and unfairness (for better and worse).
  - Warns about the dangers of regulatory capture
- **Appendix H**: Jane R. Yakowitz Bambauer, *Tragedy of the Digital Commons*, 25 HARV. J.L. & TECH 1 (2011).[16]
  - Discusses value of Big Data, both for innovation and for free expression
  - Specifically addresses how to encourage proper de-identification while minimizing the risk of harmful re-identification.

Below follow responses to some of specific questions asked by the NTIA's Request for Comments.

1. How can the Consumer Privacy Bill of Rights, which is based on the Fair Information Practice Principles, support the innovations of big data while at the same time responding to its risks?

As the Cato Institute's Jim Harper so eloquently puts it:

> Appeals to the [FIPPs] are a ceremonial deism of sorts, boilerplate that advocates use when they don't know how to give consumers meaningful notice of information

[15] *Available at* http://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00451-58007.pdf.

[16] *Available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749.

> policies, when they don't know when or how consumers should exercise choice about information sharing and use, when they don't know what circumstances justify giving consumers access to data about them, and when they don't know how to describe which circumstances—much less which systems or what levels of spending—make personal data sufficiently "secure."[17]

Whether the principles of the Consumer Privacy Bill of Rights, much like the Fair Information Practice Principles, actually make consumers better off depends on how they are transposed into law. Such a Bill of Rights will not be effective in protecting consumers unless policymakers adapt them intelligently. Policymakers must take into consideration that wholesale adoption of the FIPPs in a commercial environment impose real costs and burdens on consumers. Cost-benefit analysis should be required before any of the proposed principles are translated into law.

2. Should any of the specific elements of the Consumer Privacy Bill of Rights be clarified or modified to accommodate the benefits of big data? Should any of those elements be clarified or modified to address the risks posed by big data?

Each of the elements should be assessed through the lens of careful economic analysis before being codified in legislation.

6. The Privacy Blueprint stated:

> The Administration urges Congress to pass legislation adopting the Consumer Privacy Bill of Rights . . . Congress should act to protect consumers from violations of the rights defined in the Administration's proposed Consumer Privacy Bill of Rights. These rights provide clear protection for consumers and define rules of the road for the rapidly growing marketplace for personal data. The legislation should permit the FTC and State Attorneys General to enforce these rights directly . . . To provide greater legal certainty and to encourage the development and adoption of industry-specific codes of conduct, the Administration also supports legislation that authorizes the FTC to review codes of conduct and grant companies that commit to adhere—and do adhere—to such codes forbearance from enforcement of provisions of the legislation.

[17] Jim Harper, *Reputation Under Regulation: The Fair Credit Reporting Act at 40 and Lessons for the Internet Privacy Debate*, Cato Policy Analysis No. 690 (Dec. 8, 2011), http://www.cato.org/pubs/pas/PA690.pdf.

How can potential legislation with respect to consumer privacy support the innovations of big data while responding to its risks?

Rather than get bogged down in abstract debates about the ideal regulatory regime for privacy and data security, an intellectual quagmire in which Washington has been stuck since the FTC first endorsed comprehensive privacy legislation in 2000 (over the vigorous objections of two Commissioners),[18] this inquiry should at least begin with, if not focus on, the legal regime that currently exists for regulating Big Data and other new technologies. That means assessing not merely what the FTC has done about privacy and data security in the past but, more importantly, how it has operated.

FTC leadership increasingly point to what they call a "common law" of digital consumer protection, meaning the dozens of enforcement actions they have settled across a wide range of cases, from online fraud to data brokers to data security to user interface design. A case-by-case method does indeed have great virtues over ex ante regulation for precisely the reasons mentioned above: it is difficult to predict the future, especially the unknowable benefits of new technologies, and attempts to encode today's expectations in law often do more harm than good. As the FTC declared in its 1980 Policy Statement on Unfairness: "[Section 5 of the FTC act] was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[19]

But even if the FTC has reached the right policy outcome in many, or even most cases, its version of the "common law" is a hollow one, devoid of the very analytical rigor by which the adversarial process of litigation weighs competing theories and advances doctrine.

The FTC regulates privacy, and will regulate Big Data, primarily through its deception and unfairness powers. Yet in over seventeen years of dealing with digital consumer protection cases, the FTC has done little to develop these rich legal concepts beyond their application in the traditional marketing contexts, which the FTC was originally created to police.

This is chiefly because companies so rarely challenge enforcement actions and when the Commission settles an enforcement action, Section 5(b) requires only that (a) the

[18] http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission
[19] http://www.ftc.gov/ftc-policy-statement-on-unfairness

Commission has "reason to believe" a violation of law has occurred and (b) believes that opening the enforcement action would be in the public interest. Section 5(b) does not require any justification or process for settling a case unless the Commission seeks a monetary penalty (e.g., for violations of existing consent decrees). Thus, the settlements cited by the Commission as "guidance" do not even, by their own terms, purport to reach the merits of underlying issues. The Bureau of Economics, which has played a vital role in helping to shape what may far more accurately be called the "common law" of antitrust over the course of decades, has played little apparent role in guiding the FTC's approach to consumer protection. This has led the FTC to prioritize creative theories of harm and issues that might make compelling law review topics over clear consumer harms such as identity theft. While identity theft remains far and away the leading source of consumer complaints to the FTC,[20] the FTC has not held a workshop on the topic under this Administration.

The FTC has, commendably, begun to remedy its shortcomings in other areas, most notably by trying to build an in-house technologist capability. But it has resisted changing its overall approach for the simple, understandable reason that law enforcement agencies rarely, if ever, want to make their jobs even slightly more difficult. It is no more realistic to expect the FTC to reform its own processes without significant external pressure than it is to expect the NSA to do so. Once again, what is required is leadership from the Administration and Congress into the FTC's processes.

We believe the FTC's underlying legal standards are fundamentally sound and already provide basis for "comprehensive privacy regulation," including Big Data. But if the FTC is to be trusted with the sweeping, vague power it currently holds over nearly every company in America, it is critical that a serious inquiry begin into how the FTC operates. Clearly, the courts have failed to play the role both the FTC and Congress assumed they would when the FTC declared, in an effort to defuse a heated stand-off with an outraged Congress over the FTC's abuse its authority,[21] that:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of

[20] http://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national-consumer-complaints-2013
[21] Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, (May 30, 2003), *available at* http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

> unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'"[22]

Our FTC: Technology & Reform Project, composed of leading FTC experts and veterans, has begun an inquiry into how the FTC operates and how its processes could be improved to draw on many of the benefits of a true common law (Appendix B).[23] Like this inquiry, we see our own project as the beginning of an ongoing dialog. But already it has become clear that a series of relatively small changes could vastly improve how the FTC weighs concerns raised by new technologies, most notably ensuring clearer analysis of the component elements of its unfairness and deception powers, and greater incorporation of economics and First Amendment values in its analysis. By carefully amending Section 5 to create procedural safeguards for how the FTC settles cases and by examining why defendants essentially always settle, Congress may be able to help the FTC better execute its mission of advancing consumer welfare by focusing on clear harms to consumers that are not outweighed by greater benefits and that consumers themselves cannot effectively avoid.

Geoff Manne's attached paper (Appendix F) also explores these issues in more detail.

7. The PCAST Report states that in some cases ''it is practically impossible'' with any high degree of assurance for data holders to identify and delete ''all the data about an individual'' particularly in light of the distributed and redundant nature of data storage. Do such challenges pose privacy risks? How significant are the privacy risks, and how might such challenges be addressed? Are there particular policy or technical solutions that would

[22] http://www.ftc.gov/ftc-policy-statement-on-unfairness

[23] Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission: Report 1.0 FTC: Technology & Reform Project, (Dec. 2013) http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf

be useful to consider? Would concepts of ''reasonableness'' be useful in addressing data deletion?

As highlighted in the PCAST Report, it is often practically impossible to effectively identify and delete all the information a data holder has about an individual. Additionally, with the increasing availability of affordable data storage, the case for data retention over deletion gets even stronger.

These data retention policies do pose some privacy risks. For one, if data is retained in company servers beyond the length of an individual's commercial relationship with the company, failure to delete the data may needlessly expose it to the risk of falling into the wrong hands via a subsequent cyberattack or lapse in security. Also, even if it has been anonymized, future uses of consumer data can reveal relationships among data sets that effectively de-anonymizes the data and reveals the identity of the data subject. yes

There is likely no perfect solution for how data about an individual should be handled once the commercial relationship between the individual and the data holder has effectively ended, but some steps may be taken to address the challenges in this area. A "reasonableness" standard would be useful in this context, because asking a data holder to take all "reasonable" steps to delete the information it has about an individual is more reflective of the difficulties associated with such deletion. Anonymization of data is one way to preserve the potential utility of data while better safeguarding the privacy interests of the data subjects, but this technical solution is imperfect--much like the science of data encryption--so a potential "reasonableness" standard could also be of great use in that context.

8. The Big Data Report notes that the data services sector is regulated with respect to certain uses of data, such that consumers receive notice of some decisions based on brokered data, access to the data, and the opportunity to correct or delete inaccurate data. The Big Data Report also notes that other uses of data by data brokers ''could have significant ramifications for targeted individuals.'' How significant are such risks? How could they be addressed in the context of the Consumer Privacy Bill of Rights? Should they be? Should potential privacy legislation impose similar obligations with respect to uses of data that are not currently regulated?

This question cannot be answered without a thorough assessment of what is and is not covered by existing laws regulating credit, insurance, housing, employment, etc. and by the FTC's general Section 5 authority.

9. How significant are the privacy risks posed by unindexed data backups and other ''latent information about individuals?'' Do standard methods exist for determining whether data is sufficiently obfuscated and/or unavailable as to be irretrievable as a practical matter?

Yes, unindexed backups and other "latent information about individuals" are two forms of data that may be practically impossible for a data holder to seek out and delete in response to an individual's request to delete all associated data. That these data are comparatively obfuscated and/or irretrievable as a practical matter does not mean the risks associated with their unauthorized disclosure are negligible, as future data fusion may transform previously obfuscated data into readily identifiable information about the data subjects. But the more important questions are legal:

- What standard should govern attempts to erase such information in response to that individual's request for deletion? As discussed above in response to question 7, a "reasonableness" standard should be implemented to cover such attempts.
- How should the legal duty against re-identification be structured?

We address both questions below.

10. The PCAST Report notes that ''data fusion occurs when data from different sources are brought into contact and new, often unexpected, phenomena emerge;'' this process ''frequently results in the identification of individual people,'' even when the underlying data sources were not linked to individuals' identities. How significant are the privacy risks associated with this? How should entities performing big data analysis implement individuals' requests to delete personal data when previously unassociated information becomes associated with an individual at a subsequent date? Do existing systems enable entities to log and act on deletion requests on an ongoing basis?

This issue has already been discussed at length by both Paul Ohm, in *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*,[24] and Jane R. Yakowitz Bambauer, in *Tragedy of the Digital Commons* (Appendix G).

Yes, the possibility of re-identification creates risks for consumers, but no, contra the assumptions made by Paul Ohm and others, this does not mean anonymization of data is futile. The scholarly literature in this field, with the notable exceptions of Bambauer and Daniel Barth-Jones, generally fails to take into account the costs of re-identifying an individual from anonymized data. Not everything that can, theoretically, be done actually will, given the costs of doing so (supply side). A realistic assessment of privacy risks must take these costs into account. As Bambauer puts it:

> Like any default hypothesis, the best starting point for privacy policy is to assume that re-identification does not happen until we have evidence that it does. Because there is lower-hanging fruit for the identity thief and the behavioral marketer -- blog posts to be scraped and consumer databases to be purchased -- the thought that these personae non gratae are performing sophisticated de-anonymization algorithms is implausible.[25]

Thus, it would be unwise to stifle the significant public benefits that such data fusion techniques can produce only for the sake of protecting against purely theoretical harms. However, a reasonable prescriptive framework for handling anonymization in the data fusion context could be useful, and such a framework is discussed in the response to the next question. A particular system for responding to individual deletion requests could likely be worked into such a prescriptive framework, but any such system must incorporate a "reasonableness" standard, both as to the information to be deleted and the timeframe for processing a request.

11. As the PCAST Report explains, ''it is increasingly easy to defeat [deidentification of personal data] by the very techniques that are being developed for many legitimate applications of big data.'' However, de-identification may remain useful as an added safeguard in some contexts, particularly when employed in combination with policy safeguards. How significant are the privacy risks posed by re-identification of de-identified

[24] 57 UCLA L. Rev. 1701 (2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.
[25] Appendix G, at 39.

data? How can deidentification be used to mitigate privacy risks in light of the analytical capabilities of big data? Can particular policy safeguards bolster the effectiveness of de-identification? Does the relative efficacy of de-identification depend on whether it is applied to public or private data sets? Can differential privacy mitigate risks in some cases? What steps could the government or private sector take to expand the capabilities and practical application of these techniques?

The issues regarding re-identification of de-identified personal data are very similar to the risks posed by data fusion techniques addressed in the previous question. Along these lines, it is again worth considering the work by Paul Ohm and Jane R. Yakowitz Bambauer. As the academic literature on the subject illustrates, there are significant public interest benefits from the fusion of big data sets, and, although there are also potential harms associated with these practices, the theoretical harms rarely if ever materialize.

Much like encryption, data de-identification techniques can be beaten, but there are significant costs involved, meaning that such de-identification will be unlikely to take place in the vast majority of circumstances. Thus, if government is to take any steps to expand the capabilities and practical application of de-identification techniques, the economic calculation is really what matters, and the FTC's Bureau of Economics should first undertake a serious analysis of the costs and benefits of de-identification.

One potential model the FTC should consider is Bambauer's proposal, which has three aspects:

> (1) it clarifies what a data producer is expected to do in order to anonymize a dataset and avoid the dissemination of legally cognizable PII [Personally Identifiable Information]; (2) it immunizes the data producer from privacy-related liability if the anonymization protocols are properly implemented; and (3) it punishes with harsh criminal penalties any recipient of anonymized data who re-identifies a subject in the dataset for an improper purpose.[26]

Each of these aspects is discussed in greater length in Bambauer's article,[27] so we will touch upon them only briefly here. In this context, fear of releasing PII and having to defend

[26] *Id.* at 44.
[27] *Id.* at 44-50.

against a privacy lawsuit inhibit many researchers from sharing their datasets with one another, stifling potential innovations and new lines of research. Thus, it is important for researchers and other data producers to have clear anonymization protocols in place that can be stuck to for legal safe harbor, in order to facilitate more sharing of datasets by reducing the threat of potential liability. These protocols must also be designed so as not to be too burdensome to comply with, otherwise it will defeat the purpose of putting them into place.

The biggest concern, here, is with potential bad actors who might try to re-identify data after the fact, so imposing harsh criminal penalties upon such actions is entirely prudent. The current scheme imposes penalties upon only those who release data, and not upon the eventual end-users of the data, so a particular law to address the potential actions of the latter group is warranted.

12. The Big Data Report concludes that ''big data technologies can cause societal harms beyond damages to privacy, such as discrimination against individuals and groups'' and warns ''big data could enable new forms of discrimination and predatory practices.'' The Report states that ''it is the responsibility of government to ensure that transformative technologies are used fairly'' and urges agencies to determine ''how to protect citizens from new forms of discrimination that may be enabled by big data technologies.'' Should the Consumer Privacy Bill of Rights address the risk of discriminatory effects resulting from automated decision processes using personal data, and if so, how? How could consumer privacy legislation (either alone or in combination with anti-discrimination laws) make a useful contribution to addressing this concern? Should big data analytics be accompanied by assessments of the potential discriminatory impacts on protected classes?

These harms are already addressed by a number of laws governing discrimination in credit, lending, housing, employment, pricing, and various other eligibility decisions. Ideally, a Privacy Law Modernization Commission would conduct a comprehensive study of such laws to assess what these laws do and do not cover, what shortcomings have arisen, or be like to arise, in applying them to uses of Big Data, and what lessons can be learned from our experience with them. The PLMC would also work with the FTC's Bureau of Economics to study the underlying economics of alleged price discrimination.

13. Can accountability mechanisms play a useful role in promoting socially beneficial uses of big data while safeguarding privacy? Should ethics boards, privacy advisory committees, consumer advisory boards, or Institutional Review Boards (IRBs) be consulted when practical limits frustrate transparency and individuals' control over their personal information? How could such entities be structured? How might they be useful in the commercial context? Can privacy impact assessments and third-party audits complement the work of such entities? What kinds of parameters would be valuable for different kinds of big data analysts to consider, and what kinds of incentives might be most effective in promoting their consideration?

Such "accountability mechanisms" have an obvious emotional appeal and may well be part of the best practices that should be followed by responsible companies. But enshrining such requirements in law could raise a host of practical problems. What would such requirements mean in the rough-and-tumble world of data-driven innovation? How would start-ups cope with such a burden? This question, even more than others, cries out for careful economic analysis to ensure that such mechanisms do not become barriers to entry or stumbling blocks for the constant testing that drives perpetual refinement of the services enjoyed by consumers.

18. How can the approaches and issues addressed in Questions 14–17 be accommodated within the Consumer Privacy Bill of Rights?

This question is too complex to adequately addressed through this informal comment process. It requires the expertise, and gravitas, of an expert, bipartisan body such as we propose in the form of a Privacy Law Modernization Commission.

TECH FREEDOM

Comments of

TechFreedom[1]

In the Matter of

Government "Big Data"

Request for Information
A Notice by the Office of Science and Technology Policy

March 31, 2014

[1] TechFreedom is a a non-profit, non-partisan technology policy think tank with 501(c)(3) tax-exempt status. Questions may directed to Berin Szoka, President of TechFreedom, at bszoka@techfreedom.org.

Understanding the benefits and costs of Big Data and even beginning to weigh them against each other is likely not something that can be achieved in the limited 90-day window given to the Office of Science and Technology Policy. Mr. Podesta seemed to acknowledge this in his blog post about this inquiry:

> we expect to deliver to the President a report that anticipates future technological trends and frames the key questions that the collection, availability, and use of 'big data' raise – both for our government, and the nation as a whole. It will help identify technological changes to watch, whether those technological changes are addressed by the U.S.'s current policy framework and highlight where further government action, funding, research and consideration may be required.[2]

Above all, we urge OSTP, the Administration, and those following this inquiry to keep clearly in mind that this report is the beginning of an ongoing process, not the end, that it will frame many more questions than it can possibly answer. Even with this more limited ambition, the Report can offer invaluable guidance to policymakers struggling to understand Big Data and what, if anything, to "do" about it.

Economics Must Guide Any Study of Big Data

On the benefits of Big Data, we urge OSTP to keep in mind two cautions. First, Big Data is merely another trend in an ongoing process of disruptive innovation that has characterized the Digital Revolution. Even before the advent of the Internet, the semiconductor industry saw change accelerate at a pace that was scarcely before conceivable. We now know that this was Moore's Law at work: the doubling of computing power roughly every eighteen months. One industry after another has been disrupted by digital technologies, which allow new companies to emerge out of nowhere with new ways of doing things that can quickly render obsolete not just existing companies but existing ways of doing business – and radically change consumer expectations.[3]

---

[2] http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy

[3] *See generally* Larry Downes & Paul Nunes, *Big Bang Disruption: Strategy in the Age of Devastating Innovation* (2014).

In hindsight, the benefits to consumers of this topsy-turvy process loom large in many aspects of American life. Yet the process has been painful, not just for incumbent industries and business models, but for those uncomfortable with "What Hath [Technology] Wrought"[4] in our daily lives, from transforming media to unsettling our most deeply held assumptions about privacy, security, child-rearing and a host of other emotionally wrought topics. The only safe generalization that can be made is that, however difficult these changes may seem to us in hindsight, we tend to forget how painful they were at the time, both because it was difficult for even experts to predict the benefits of new technologies and because risk aversion so is deeply rooted in human nature that few at the time would really have believed even the most accurate predictions that it was worth it. Had "the future" been put up for a vote, it probably would have been banned. The point is that any inquiry into future benefits should begin from the assumption that many of the greatest benefits remain unknowable *ex ante* and that any attempt to weigh unknown future benefits against more easily imaginable potential harms will fundamentally bias policymakers against innovation.

Second, cost-benefit analyses generally, and especially in advance of evolving technologies, tend to operate in aggregates because those are more easily measured: How large an economic boost might Big Data make to our society? What are the current costs of, say, identity theft? These predictions can be useful for providing directional indications of future trade-offs, but they should not be mistaken for anything more than that. Life operates, at all levels, not in terms of aggregate, but on the margin: aggregate benefits tell us little about the trade-offs involved in specific practices, and where regulation can be most helpful – or harmful.

These two cautions should lead this inquiry to begin from a stance of humility and a general presumption that we are limited in our ability both to predict and to shape the future in ways that will actually benefit consumers. The task of economics is not to make specific predictions so that policymakers can pull "policy levers" with a clear sense of what the resulting effect of their manipulations will be, but, as Friedrich Hayek famously put it, "to demonstrate to men how little they really know about what they imagine they can design."

Economics *can* play a vital role in this inquiry, however, if assessment of trade-offs on the margins is integrated throughout, even in topics that may seem to have little to do with economics. Nowhere is economics more sorely needed than in the debate over the efficacy

[4] "What hath God wrought," a phrase from the Book of Numbers, was the first message transmitted by telegraph in 1844.

of de-identification, which is in fact a debate over the cost-effectiveness of re-identification. It is not enough to assert that a data set *can* be re-identified. After all, "Three monkeys hitting keys at random on typewriters for an infinite amount of time will almost surely produce Hamlet."[5] The key question is: is a particular data set *likely* to be re-identified based on the potential value of the uses of the data and the costs of re-identification. In other words, how many monkeys and how long *would* it take? And on the other end, how much de-identification is adequate is also as much an economic question as it is a computer science or statistical question.[6]

An economics-informed assessment of these trade-offs should lead us to more carefully weigh the costs and benefits of large data sets and to focus regulation, and the limited enforcement resources of regulators, on areas where regulation can do more good than harm. This is true on most, if not all, of the concerns raised by Big Data, from privacy to data security. Economics can help understand the trade-offs involved in addressing "non-economic" concerns like societal and constitutional values. Even if economists do not have the final word on policy decisions, they have an invaluable role to play as advisors.

Big Data *Is* Speech: This Inquiry Must Address the First Amendment

Since the purpose of this inquiry is, in the end, to shape policymaking, it must also confront another dimension of trade-offs: regulation of the private sector's use of "Big Data" largely means regulation of speech protected by the First Amendment. The Supreme Court made clear in *Sorrell v. IMS Health, Inc.*, 131 S. Ct. 2653 (2011) that data *is* speech:

> This Court has held that the **creation and dissemination of information are speech** within the meaning of the First Amendment. See, e.g. , Bartnicki , supra , at 527 ("[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct" (some internal quotation marks omitted)); Rubin v. Coors Brewing Co. , 514 U. S. 476, 481 (1995) ("information on beer labels" is speech); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc. , 472 U. S. 749, 759 (1985) (plurality opinion) (credit report is

[5] David Ives, *Words, Words, Words* (1987).

[6] See generally, Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. Jrnl. Law & Tech 1 (2011), http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech1.pdf

> "speech"). Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.
>
> The State asks for an exception to the rule that **information is speech**...[7]

It is by no means clear how the Court's jurisprudence on First Amendment protection will evolve. The Court has *always* struggled to apply free speech principles as technology has changed, and Big Data will, in that respect, be much like the telegraph, telephone, film, television, the Internet and video games. Given that OSTP's competence is technical rather than legal, this inquiry, and the future studies it engenders, should focus on the forms of "speech" enabled by Big Data and how it might "advance human knowledge" within its overall inquiry into the benefits of Big Data. This will help policymakers to approach Big Data with greater caution than they have traditionally approached new media.

This does not necessarily mean *less* regulation but does mean *better* and more constitutionally defensible regulation. Even those who think the government should have a lower burden in regulating Big Data than it would in regulating speech more generally should find the general approach of First Amendment analysis a useful heuristic for thinking about how best to deal with Big Data: What, exactly, is the government's interest? How substantial is it? Are the means chosen appropriately or narrowly tailored to address that interest? Are they over-broad? Are there other, less restrictive means available to address the problem? Is the approach either over- or under-inclusive?[8]

These are difficult questions that will either be dealt with carefully by policymakers or, if not, by courts who send legislators back to the drafting board. This inquiry cannot, of course, address all of them, but it must begin the process of integrating an assessment of First Amendment values and doctrines, along with economics, into the study of Big Data and its policy implications.

---

[7] 131 S. Ct. at 2667.

[8] See generally Berin Szoka, The Progress & Freedom Foundation, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, Comments to the FTC Privacy Roundtables (Dec. 7, 2009), available at http://www.scribd.com/doc/22384078/PFF-Comments-on-FTC-Privacy-Workshop-12-7-09

Government Threats to Privacy

The low-hanging fruit for this inquiry – the areas where policymakers can do the greatest good at the lowest cost in terms of lost innovation, economic benefits or meddling in the still-evolving speech platforms of the Digital Age – is clear: focus on government. Government is not the only source of harm to consumers, but it is the source of the greatest and clearest harms.

Long before Edward Snowden's revelations, TechFreedom and dozens of other non-governmental civil liberties organizations, trade associations and companies joined together in the Digital Due Process Coalition to advance four simple principles for reforming the Electronic Communications Privacy Act of 1986.[9] A clear, broad consensus now exists around the need to ensure that law enforcement agencies cannot access content without a warrant. Indeed, the Sixth Circuit has even ruled that ECPA's failure to require a warrant for content in general violates the Fourth Amendment's protection against unreasonable searches and seizures.[10] Essentially the entire court in *U.S. v. Jones* clearly indicated their discomfort with the failure of our laws to protect Fourth Amendment values as technology has changed.[11] Justice Sotomayor warned that "Awareness that the Government may be watching chills associational and expressive freedoms" and called for the Court "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Justice Alito and three other Justices explicitly called on Congress to address "concern about new intrusions on privacy" through legislation because Chief Justice Taft's warning that "regulation of wiretapping was a matter better left for Congress has been borne out."

Yet, four years later, while the courts have made great progress, including a scathing magistrate decision scolding the Department of Justice for not meaningfully complying with *Warshak*,[12] Congress has talked about the issue but has done nothing – but at least action

---

[9] http://digitaldueprocess.org/index.cfm?objectid=A77781D0-2551-11DF-8E02000C296BA163

[10] *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2011).

[11] *U.S. v. Jones*, 565 U.S. 945 (2012).

[12] In Matter of United States of America for a Search Warrant for a Black Kyocera Corp Model C5170 Cellular Telephone with FCC ID: V65V5170 (D.D.C. March 7, 2014), available at https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2014mj0231-2

finally appears imminent: ECPA Reform legislation now has 193 sponsors in the House.[13] This momentum towards long overdue reform has built slowly but steadily – with no help whatsoever from this Administration.

It takes a special kind of temerity for the President to loftily promise a "Consumer Privacy Bill of Rights"[14] – while doing nothing to protect the *real* Bill of Rights, the Fourth Amendment that is the crown jewel of the civil liberties: the warrant requirement that was among the chief inspirations for the American Revolution.[15]

This Administration's Department of Justice has sought warrants for email content only when ordered to do so by the Sixth Circuit in *Warshak* and even then, did not take the requirement seriously, as the recent magistrate decision makes scathingly clear. Worse, the Administration has actively worked to sabotage ECPA reform by orchestrating opposition to ECPA reform from nominally independent agencies, which appear in fact to be working in conjunction with the Department of Justice. In particular, the fanatic insistence by the Securities and Exchange Commission, now joined by the Federal Trade Commission and other agencies, that administrative agencies should be exempt from the general requirement for a warrant to access content information, has stalled ECPA reform in the Senate.

Meanwhile, the Administration has simply ignored a WhiteHouse.gov petition signed by 110,423 Americans entitled "Reform ECPA: Tell the Government to Get a Warrant."[16] Despite promising to respond "in a timely fashion" to any petition that receives 100,000 signatures within 30 days,[17] the Administration has done nothing[18] – yet it has found plenty of time to respond to a petition by *Star Wars* fans urging the Administration to begin building a Death

---

[13] H.R. 1852: Email Privacy Act, https://www.govtrack.us/congress/bills/113/hr1852

[14] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[15] See Testimony of Berin Szoka, TechFreedom, before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade, hearing on *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?*, at 4-5, March 29, 2012, available at http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Szoka-CMT-Balancing-Privacy-and-Innovation-President-Proposal-2012-3-29.pdf

[16] https://petitions.whitehouse.gov/petition/reform-ecpa-tell-government-get-warrant/nq258dxk

[17] https://petitions.whitehouse.gov/how-why/terms-participation

[18] Mark Stanley, Center for Democracy & Technology, *White House Still Silent on Warrantless Email Snooping*, March 31, 2014, https://cdt.org/blogs/mark-stanley/3103white-house-still-silent-warrantless-email-snooping

Star by 2016 with the clever title "This Isn't the Petition Response You're Looking For."[19] We are *not* amused.

This stubborn opposition to sensible, bi-partisan privacy reform is outrageous and shameful, a hypocrisy outweighed only by the Administration's defense of its blanket surveillance of ordinary Americans – a problem so well known that it requires no special description here.

It's time for the Administration to stop dodging responsibility or trying to divert attention from the government-created problems by pointing its finger at the private sector, by demonizing private companies' collection and use of data while the government continues to flaunt the Fourth Amendment.

This inquiry offers the Administration a chance to redeem itself, at least in part. This report should assess the full costs, both in economic terms and in constitutional values, of easy surveillance and access to private data by law enforcement and national security agencies. The report should recommend ECPA reform as outlined by the Digital Due Process Coalition, especially a clear email requirement for access to content and location data that applies to *all* law enforcement agencies, including regulators. OSTP's report should support real and meaningful reforms to national security agencies' collection of, and access to, private communications, both their content and metadata.

Regulating the Private Sector

Getting government's own house in order does not mean ignoring legitimate concerns raised by Big Data, such as how privacy companies may use data they collect and how they secure it against breaches. This inquiry can proceed along both tracks. But rather than get bogged down in abstract debates about the ideal regulatory regime for privacy and data security, an intellectual quagmire in which Washington has been stuck since the FTC first endorsed comprehensive privacy legislation in 2000 (over the vigorous objections of two Commissioners),[20] this inquiry should at least begin with, if not focus on, the legal regime that currently exists for regulating Big Data and other new technologies. That means assessing not merely what the FTC has done about privacy and data security in the past but, more importantly, *how* it has operated.

---

[19] https://petitions.whitehouse.gov/response/isnt-petition-response-youre-looking

[20] http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission

FTC leadership increasingly point to what they call a "common law" of digital consumer protection, meaning the dozens of enforcement actions they have settled across a wide range of cases, from online fraud to data brokers to data security to user interface design. A case-by-case method does indeed have great virtues over *ex ante* regulation for precisely the reasons mentioned above: it is difficult to predict the future, especially the unknowable benefits of new technologies, and attempts to encode today's expectations in law often do more harm than good. As the FTC declared in its 1980 Policy Statement on Unfairness: "[Section 5 of the FTC act] was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[21]

But even if the FTC has reached the right policy outcome in many, or even most cases, its version of the "common law" is a hollow one, devoid of the very analytical rigor by which the adversarial process of litigation weighs competing theories and advances doctrine.

The FTC regulates privacy, and will regulate Big Data, primarily through its deception and unfairness powers. Yet in over seventeen years of dealing with digital consumer protection cases, the FTC has done little to develop these rich legal concepts beyond their application in the traditional marketing contexts, which the FTC was originally created to police.

This is chiefly because companies so rarely challenge enforcement actions and when the Commission settles an enforcement action, Section 5(b) requires only that (a) the Commission has "reason to believe" a violation of law has occurred and (b) believes that *opening* the enforcement action would be in the public interest. Section 5(b) does not require *any* justification or process for *settling* a case unless the Commission seeks a monetary penalty (e.g., for violations of existing consent decrees). Thus, the settlements cited by the Commission as "guidance" do not even, by their own terms, purport to reach the merits of underlying issues. The Bureau of Economics, which has played a vital role in helping to shape what may far more accurately be called the "common law" of antitrust over the course of decades, has played little apparent role in guiding the FTC's approach to consumer protection. This has led the FTC to prioritize creative theories of harm and issues that might make compelling law review topics over clear consumer harms such as identity theft. While

[21] http://www.ftc.gov/ftc-policy-statement-on-unfairness

identity theft remains far and away the leading source of consumer complaints to the FTC,[22] the FTC has not held a workshop on the topic under this Administration.

The FTC has, commendably, begun to remedy its shortcomings in other areas, most notably by trying to build an in-house technologist capability. But it has resisted changing its overall approach for the simple, understandable reason that law enforcement agencies rarely, if ever, want to make their jobs even slightly more difficult. It is no more realistic to expect the FTC to reform its own processes without significant external pressure than it is to expect the NSA to do so. Once again, what is required is leadership from the Administration and Congress into the FTC's processes.

We believe the FTC's underlying legal standards are fundamentally sound and already provide basis for "comprehensive privacy regulation," including Big Data. But if the FTC is to be trusted with the sweeping, vague power it currently holds over nearly every company in America, it is critical that a serious inquiry begin into *how* the FTC operates. Clearly, the courts have failed to play the role both the FTC and Congress assumed they would when the FTC declared, in an effort to defuse a heated stand-off with an outraged Congress over the FTC's abuse its authority,[23] that:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, **subject to judicial review**, in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court

[22] http://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national-consumer-complaints-2013

[23] Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, May 30, 2003, http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection

> elsewhere has called 'the **gradual process of judicial inclusion and exclusion**.'"[24]

Our FTC: Technology & Reform Project, composed of leading FTC experts and veterans, has begun an inquiry into how the FTC operates and how its processes could be improved to draw on many of the benefits of a true common law. [25] Like this inquiry, we see our own project as the beginning of an ongoing dialog. But already it has become clear that a series of relatively small changes could vastly improve how the FTC weighs concerns raised by new technologies, most notably ensuring clearer analysis of the component elements of its unfairness and deception powers, and greater incorporation of economics and First Amendment values in its analysis. By carefully amending Section 5 to create procedural safeguards for how the FTC settles cases and by examining why defendants essentially *always* settle, Congress may be able to help the FTC better execute its mission of advancing consumer welfare by focusing on clear harms to consumers that are not outweighed by greater benefits and that consumers themselves cannot effectively avoid.

OSTP's inquiry offers an invaluable opportunity to refocus the endless, unconstructive "privacy debate" on the concrete "how" of privacy law: FTC process. This, more than any abstract legal theory, will ultimately shape the regulation of Big Data.

---

[24] http://www.ftc.gov/ftc-policy-statement-on-unfairness

[25] *Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission: Report 1.0 FTC: Technology & Reform Project*, (Dec. 2013) http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf

Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission

December 2013

Report 1.0 of the
FTC: Technology & Reform Project

Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission

December 2013

Report 1.0 of the FTC:
Technology & Reform Project

This document represents the combined input of several authors and commentators, and has been compiled to ask questions and prompt discussion about the Federal Trade Commission. It is, by design, over-inclusive, so that it may foster broad discussion. At the same time, it is also certainly not complete. This document does not necessarily represent the views of its principal authors or other contributors to the drafting process, nor the members of the FTC: Technology & Reform Project. The FTC: Technology & Reform Project was convened by the International Center for Law & Economics and TechFreedom. It is not affiliated in any way with the FTC.

I. Introduction

In 1914, Congress gave the FTC sweeping jurisdiction and broad powers to enforce flexible rules, to ensure that it would have the ability to serve as the regulator of trade and business that Congress intended it be. Much, perhaps even the great majority, of what the FTC does is uncontroversial and is widely supported, even by critics of the regulatory state. However, both Congress and the courts have expressed concern about how the FTC has used its considerable discretion in some areas, particularly in its evolving interpretation of "unfairness." Now, as the FTC approaches its 100th anniversary, the FTC, courts and Congress face a series of decisions about how to apply or constrain that discretion. These questions will become especially pressing as the FTC uses is its authority in new ways, expands its authority into new areas, or gains new authority from Congress.

The purpose of this report is not to lambaste the agency, but rather to ask to ask whether more should be done to improve how the agency exercises its discretion, and, if so, how to do so without hamstringing the agency. Indeed, improving the well-considered constraints on the FTC's use of its discretion may make the Commission more, not less, effective by bringing about clearer, more consistent guidance, in turn increasing the FTC's credibility and achieving greater compliance. Ultimately, the measure of the FTC's success should not be how "active" it is, how far it extends its jurisdiction or how far it pushes the boundaries of its discretion, but rather how well it achieves its overarching purpose of maximizing consumer welfare.

Specific recommendations for reform will be evaluated in future reports, but this this report is an essential predicate to the reform process, framing the questions, both about institutional processes and dynamics and about discrete areas, including privacy, advertising, patents, and merger enforcement. In particular, the report highlights two specific areas in which the FTC's exercise of its discretion has become increasingly controversial: the FTC's data security and privacy cases, and its Unfair Methods of Competition (UMC) cases. Both of these sets of cases involve the core question of how to define unfairness under Section 5 of the FTC Act (Section 5), a question that the FTC itself grappled with in writing its Unfairness Policy Statement of 1980:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'"[1]

This report focuses not so much on what such underlying criteria ought to be or on the right outcome in any particular area of law. Instead, it focuses on the fundamental need for such limiting "criteria" under

[1] Letter from the FTC to the House Consumer Subcommittee, *appended to* In re International Harvester Co., 104 F.T.C. 949, 1073 (1984), *available at* http://www.ftc.gov/ftc-policy-statement-on-unfairness [hereinafter, "Unfairness Statement"].

Section 5 and the difficult question of why they have not "develop[ed] over time" in the analytically rigorous way that the courts, informed by economics, have developed the principles of antitrust law. Ultimately, the "evolutionary process" by which the laws enforced by the FTC "evolve" may be more important than what the law happens to be in a particular area at a particular point in time.

Nowhere is this form of flexibility more needed than to keep pace with the evolution of technology and changing business models and practices. Inherent limitations on anyone's knowledge about the future nature of technology, business and social norms caution skepticism as regulators attempt to predict whether any given business conduct will, on net, improve or harm consumer welfare. In fact, a host of factors suggests that even the best-intentioned regulators may tend toward overconfidence and the erroneous condemnation of novel conduct.[2] At the same time, business generally succeeds by trial-and-error more than theoretical insights or predictive power,[3] and over-regulation thus risks impairing experimentation, an essential driver of economic progress. As a consequence, doing nothing may sometimes be the best policy, and limits on regulatory discretion to act can be of enormous importance.[4]

The FTC must always weigh the costs of intervention against the costs of doing nothing. But what, and who, will limit the FTC's discretion in assessing these trade-offs? It is the same age-old question: Who will watch the watchers?

This report explores these concerns largely through the lens of technology-related issues for two reasons. First, it is in this context that the FTC has, in recent years, most assertively pushed the boundaries of its discretion. Second, even if technology issues remain a small portion of what the agency does, by slow accretion the FTC is nevertheless gradually becoming the Federal *Technology* Commission – the *de facto* regulator of a wide range of what are commonly viewed as "technology" issues that permeate the American economy. Further, Congress may give the agency additional authority over tech-related issues, such as privacy, data security, and telecommunications matters traditionally regulated by the Federal Communications Commission.

The FTC may well be the most appropriate regulator of these issues; indeed, it operates under what is almost certainly a better regulatory model than that of the FCC, for example.[5] But as the economic importance of advanced technology increases, and as the FTC's focus on technology issues grows, so too

---

[2] *See, e.g.,* Ronald H. Coase, *Industrial Organization: A Proposal for Research*, *in* ECONOMIC RESEARCH: RETROSPECT AND PROSPECT VOL. 3: POLICY ISSUES AND RESEARCH OPPORTUNITIES IN INDUSTRIAL ORGANIZATION (Victor R. Fuchs, ed. 1972), *available at* http://www.nber.org/chapters/c7618.pdf; Frank H. Easterbrook, *The Limits of Antitrust*, 63 TEX. L. REV. 1 (1984); Geoffrey A. Manne & Joshua D. Wright, *Innovation and the Limits of Antitrust*, 6 J. COMPETITION L. & ECON. 153 (2010).

[3] *See* Armen Alchian, *Uncertainty, Evolution, and Economic Theory*, 58 J. POL. ECON. 211 (1950).

[4] As Nobel Laureate economist Ronald Coase put it, "direct governmental regulation will not necessarily give better results than leaving the problem to be solved by the market or the firm. But equally there is no reason why, on occasion, such governmental administrative regulation should not lead to an improvement in economic efficiency…. There is, of course, a further alternative which is to do nothing about the problem at all." Ronald H. Coase, *The Problem of Social Cost*, 3 J. LAW & ECON. 1, 18 (1960).

[5] *See, e.g.*, Berin Szoka & Geoffrey A. Manne, *The Second Century Of The Federal Trade Commission*, TECHDIRT (Sept. 26, 2013), http://www.techdirt.com/blog/innovation/articles/20130926/16542624670/second-century-federal-trade-commission.shtml.

does the importance of understanding the scope of the FTC's discretion, and the appropriate mechanisms for limiting it where needed.

A. What this Report is About

The issues discussed here, therefore, apply broadly and suggest general areas for investigating the FTC's approach and avenues for contemplating reforms of how it operates. The FTC has in the past recognized the need to adjust both the process and the substance of traditional antitrust law to meet changing times. The same need now also confronts the Commission in a number of areas: defining unfair methods of competition beyond the traditional antitrust laws; key aspects of consumer protection law, as well as applying existing definitions with renewed vigor; and the enforcement of codes of conduct and other non-governmental sources of law as an especially crucial mechanism for flexibly governing new technologies.

This report introduces the FTC and provides a conceptual organization for major questions about how the FTC works. Our goal at this stage is to not to *answer* these questions, but to prompt discussion within a useful framework. For those steeped in the work of agencies like the FTC, this report is more analogous to a Notice of Inquiry than to a Notice of Proposed Rulemaking or Final Rule.

The report is intended to guide anyone who cares about the future of the FTC and of competition and consumer protection law more generally, regardless of her opinion on any particular controversy. The members of the FTC: Technology & Reform Project intend to offer recommendations for possible reforms to the Commission's substantive, procedural, and institutional design elsewhere during the course of this 100th year of the FTC's existence.

Organizationally, the remainder of this introduction provides some historical background and context for the FTC and the questions asked in the rest of this report. Part II considers what has emerged as a general theme as this project has developed: the nature and extent of FTC discretion. Parts III and IV develop and present questions about the Commission's work and power, with Part III focusing on general institutional and process issues and Part IV looking at specific subject matter issues.

B. The (Not-So-Unique) Role of Technology

In this report we pay particular attention to issues raised by new technology. The effect of FTC action on technology issues, companies or industries is not a fundamentally different or unique kind of problem. FTC regulation of any industry with dynamic competition and pervasive innovation increases the probability of regulatory error and the magnitude of the resulting error costs. (Indeed, because technology has transformed nearly every industry, technology regulation does affect every industry.) As such, the technology-driven issues this report focuses on are simply one manifestation of the more general issues regarding how the FTC operates and that should, potentially, be reformed.

But technology does present unique – or perhaps just especially exigent – challenges for regulators precisely because it tends to create new consumer protection and competition issues, or upset previously settled issues, and because such change tends to occur more rapidly than in some other settings. Regulation abhors a vacuum; technology tends to render existing regulation obsolete, creating such a vacuum. Moreover, technology can give rise to *new* issues, or at least *new-seeming* issues, which can leave regulators looking for novel regulatory tools and justifications for regulation. That is, regulators often feel the need to do *something*, even where it is unclear whether or what regulation is needed.

It is on the cutting edge, new issues that the stress-points in the FTC's general approach become most clearly visible, but these stress-points are by no means unique to the technological setting. Moreover, of particular importance, welfare-enhancing innovation is not just about technological advance, but also organizational, business model and contractual developments, and these important advances can also be threatened by the excessive use of discretion.[6]

Many of the FTC's most significant recent cases exemplify these concerns. Facing novel data security questions, the agency has pushed the bounds of its UDAP authority to constrain firms trying to experiment and adapt in the face of developing technology. Similarly, by expressing myriad concerns about business methods and practices in high-tech firms – among them Intel, N-Data, Rambus, Twitter, Google and Facebook – and investigating issues ranging from privacy to search engine design to patent enforcement to integrated circuit fabrication, the Commission has pushed the bounds of its Section 5 authority, and has indicated its desire to continue expanding the power afforded by that authority. In short, any large (that is, successful and innovative) firm operating in the technology sector, would be prudent to expect that today the FTC is investigating its business practices.

C. Some Historical Context: Constraining & Reasserting FTC Power

Unease about the scope of the Commission's authority is not new. The FTC was created in response to concerns that the courts were taking a too-narrow view of the antitrust laws and that Congress moved too slowly to keep up with evolving business practices. Whether that concern was warranted at the time is beyond the scope of this report, but it is clear that Congress expressly gave the Commission extremely broad and flexible powers. Over time, these powers have waxed and waned as the agency has asserted them more or less broadly and the courts and Congress have occasionally constrained them.

Since 1914, the FTC has been responsible for protecting consumers against "unfair methods of competition" (UMC). This has generally meant enforcing the same antitrust laws enforced by the Department of Justice, state attorneys general and private plaintiffs. In 1938, Congress gave the FTC additional authority to protect consumers from unfair or deceptive acts or practices (UAP or DAP or, together, UDAP). Some select history of both UDAP and UMC authority is important for informed consideration of the Commission's authority, especially regarding the concept of unfairness common to UMC and UAP.

1. UAP Authority, and How the FTC Lost Its Groove (and Its Funding)

The most important era of the FTC's UAP authority was 1972 through 1980, during which the FTC is generally recognized as having run amok with its unfairness authority. In 1964 the FTC defined unfair acts or practices by a three-part test, under which it would proscribe conduct that 1) "offends public policy," as divined from "statutes, the common law, or otherwise"; 2) "is immoral, unethical, oppressive, or unscrupulous;" or 3) "causes substantial injury to consumers (or competitors or other businessmen)."[7] The last time the Supreme Court opined on unfairness – and even then, only in dicta –

[6] *See, e.g.*, Manne & Wright, *Innovation*, *supra* note **Error! Bookmark not defined.**; Ernest Gellhorn, & William E. Kovacic, *Analytical Approaches and Institutional Processes for Implementing Competition Policy Reforms by the Federal Trade Commission.*

[7] J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, §II.A, *available at* http://www.ftc.gov/speeches/beales/unfair0603.shtm.

was its 1972 *Sperry v. Hutchinson* decision. There the Court seemed to endorse the FTC's broad understanding of unfairness, ruling that the FTC may, "like a court of equity, consider[] public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws."[8]

The FTC subsequently tested the limits of the unfairness doctrine through a rash of expansive actions. As Howard Beales, then Bureau of Consumer Protection (BCP) director, explained in a landmark 2003 historical survey, "[e]mboldened by the Supreme Court's dicta, the Commission set forth to test the limits of the unfairness doctrine. Unfortunately, the Court gave no guidance to the Commission on how to weigh the three prongs – even suggesting that the test could properly be read disjunctively."[9] In response to the FTC's rulemaking spree – and to address questions about the FTC's rulemaking authority – Congress imposed various procedural requirements on UAP-related rulemaking, beyond those of ordinary APA requirements, with the Magnuson-Moss Act of 1975.[10] But these did little to stem the FTC's efforts. "The result was a series of rulemakings relying upon broad, newly found theories of unfairness that often had no empirical basis, could be based entirely upon the individual Commissioner's personal values, and did not have to consider the ultimate costs to consumers of foregoing their ability to choose freely in the marketplace."[11] Things came to a head when, Beales explains, the FTC

> [T]ried to use unfairness to ban all advertising directed to children on the grounds that it was "immoral, unscrupulous, and unethical" and based on generalized public policies to protect children. [The FTC Chairman] opined that the Commission could use unfairness, *inter alia*, to regulate the employment of illegal aliens and to punish tax cheats and polluters.
>
> The breadth, overreaching, and lack of focus in the FTC's ambitious rulemaking agenda outraged many in business, Congress, and the media. Even the Washington Post editorialized that the FTC had become the "National Nanny…."[12]

Early in 1980, Congress passed the FTC Improvements Act, imposing further procedural safeguards on Magnuson-Moss rulemakings. President Carter declared, "This bill contains some valuable features patterned after my program to eliminate excessive regulation. It requires that FTC rules be based on sound economic analysis. Another provision directs the agency to find the least burdensome way of achieving its goals."[13] Leaders of a heavily Democratic Congress continued pressuring the FTC to limit its unfairness discretion. When, later in 1980, the FTC's funding ran out during the first modern government shutdown, Congress simply let the agency close. The FTC got the message, and in December it published the Unfairness Policy Statement in a letter to Congressional leaders, defining unfair acts or practices as those that (1) cause, or are likely to cause, substantial injury to consumers (2) that are not outweighed by countervailing benefit and (3) that consumers themselves cannot reasonably avoid.[14] Consistent with its new spirit of restraint, the FTC issued an analogous Deception Policy Statement in

[8] FTC v. Sperry & Hutchinson Co., 405 U.S. 233 (1972).

[9] Beales, *supra* note 7, at §II.A.

[10] 15 U.S.C.A. §§ 2301-2312 (2012).

[11] Beales, *supra* note 7, at §II.A.

[12] *Id.* at §II.B.

[13] Jimmy Carter, *Federal Trade Commission Improvements Act of 1980 Statement on Signing H.R. 2313 Into Law* (May 28, 1980), *available at* http://www.presidency.ucsb.edu/ws/?pid=44790.

[14] Unfairness Statement, *supra* note 1.

1983, defining deception as (1) misleading statements or omissions (2) that are material to consumer choice.[15]

The FTC had finally – under duress – agreed to limit its discretion. The Commission continued to bring enforcement actions predicated on unfairness, but further narrowed its understanding of unfairness to focus on the three-part test codified by Congress in 1994[16] (abandoning "public policy" as an independent basis) and ceased conducting new rulemakings based on unfairness. Meanwhile, unfairness slumbered as an independent basis for policing competition.

2. UMC, and How the FTC Lost That Groove, Too

The FTC's UMC authority has long been understood to give it authority to enforce the antitrust laws (*e.g.*, the Sherman and Clayton Acts). The history of this power, therefore, is largely coextensive with that of the antitrust laws. For most of the 20th century, antitrust law was very favorable to plaintiffs, with the Supreme Court recognizing a wide range of business practices as *per se* illegal, unfettered by requirements that a given practice, or practitioner of that practice, actually (or even be likely to) harm competition.[17] As a result, the FTC had little reason to push the envelope of its Section 5 UMC authority beyond the courts' interpretation of the Sherman and Clayton Acts.

This approach to antitrust law began to change in the 1970s. The generally accepted watershed moment was the publication of Robert Bork's book, THE ANTITRUST PARADOX, in 1978. THE ANTITRUST PARADOX made the case that antitrust law should be based on rigorous economic analysis – and that the subject of that analysis should be protecting consumer welfare. While the Chicago School had long criticized the course of antitrust law for its lack of economic rigor, Bork's book largely marked the beginning of the modern era of antitrust, which has seen a sweeping transition in Supreme Court precedent under which most cases are now decided under a *rule of reason* standard – a standard under which plaintiffs generally face the burden of demonstrating that conduct harms consumers and courts weigh its likely costs against its benefits.

One of the central themes of the modern era of antitrust can be characterized as "regulatory humility": Regulators should intervene in markets only with great caution. Several reasons urge such caution. First, the regulator's natural inclination – in fact, his very job – is to *regulate*. This inclination on the regulator's part is compounded by the fact that, as Ronald Coase explained,

> If an economist finds something – a business practice of one sort or another – that he does not understand, he looks for a monopoly explanation. And as in this field we are very ignorant, the number of ununderstandable practices tends to be very large, and the reliance on a monopoly explanation, frequent.[18]

[15] *See* Letter from the FTC to the Committee on Energy and Commerce, *appended to* Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984) http://www.ftc.gov/ftc-policy-statement-on-deception [hereinafter, "Deception Statement"].

[16] In 1994, Congress enshrined this statement in Section 5(n) of the FTC Act. 15 U.S.C.A. § 45(n) (2012).

[17] *See* Frank H. Easterbrook, *Is There a Ratchet in Antitrust Law?*, 60 TEX. L. REV. 705, 715 (1982).

[18] Coase, *Industrial Organization*, *supra* note **Error! Bookmark not defined.**, at 59.

Second, the greatest pressure for regulatory intervention against a firm often comes from that firm's competitors, which seek to use regulation to benefit themselves (not consumers). Many antitrust practitioners refer to this as "the first rule of antitrust": competitor complaints indicate a *competitive* market. Third, even where regulatory intervention may be justified, it is often not clear what intervention is appropriate to the harms, especially in markets characterized by rapid change or innovation. Much of the history of antitrust regulation is a catalog of failure – efforts that too often harmed the very consumers they were meant to protect.

Last, and perhaps most important, market forces often constrain harmful conduct more effectively than regulation. In competitive markets, a firm's competitors will respond to its conduct. In uncompetitive markets, the monopoly profits extracted by the malfeasant firm will attract entry by competitors eager to share in the surplus. Such market responses may not offer a perfect response to harmful conduct. But they need not be perfect to be preferable to regulation – only better than the also imperfect regulatory alternative.[19] Given the possibility that seemingly harmful conduct may, in fact, not be harmful, the difficulty of remedying harmful conduct, and the possibility that the remedy could actually harm competition and consumers, it is frequently the case that regulatory inaction is preferable to ill-conceived regulation.

Generally, this approach to analyzing competition concerns is called the "error cost" framework. Such a framework seeks to balance the potential harms of false positives (erroneous intervention) and negatives (erroneous restraint) – so-called Type 1 and Type 2 errors – against the potential benefits of correct judgments.[20] The error cost approach has come to dominate antitrust over the past 35 years. There is, however, constant pressure for antitrust law to take a more aggressive stance towards potentially harmful conduct. Yet the Supreme Court has consistently held antitrust to the more circumspect approach advocated in THE ANTITRUST PARADOX.

Because the courts for many years employed an expansive view of antitrust liability, the FTC had little reason to apply its UMC authority more expansively for much of its history. As antitrust law began to shift toward the "rule of reason," the FTC began, in the 1980s, to push the boundaries of its UMC authority beyond the traditional antitrust laws in a trio of cases.[21] However, the FTC's position was roundly rejected by the courts. Advocates for a more expansive approach to antitrust law generally have continued to advocate the view that Section 5 incorporates, but expands beyond, the "antitrust laws," however.[22]

3. Re-asserting Unfairness Authorities, or, How the FTC Is Getting Its Groove Back

Over the past decade, the FTC has begun to reassert its twin unfairness authorities. In 2000, the FTC declared that Section 5 was inadequate to address the challenges raised by digital privacy issues and

[19] *See* Coase, *Problems of Social Cost*, *supra* note **Error! Bookmark not defined.**.

[20] *See, e.g.*, Manne & Wright, *Innovation*, *supra* note **Error! Bookmark not defined.**.

[21] *See* E.I. duPont de Nemours & Co. v. FTC, 729 F.2d 128 (2d Cir. 1984); Boise Cascade v. FTC, 637 F.2d 573 (9th Cir. 1980); Official Airline Guides v. FTC, 630 F.2d 920 (2d Cir. 1980).

[22] For an informative discussion on the FTC's UMC authority and Commissioner Wright's call for more guidance from a variety of perspectives, see Truth on the Market Blog Symposium on UMC (Aug. 1-2, 2013), http://truthonthemarket.com/category/umc-symposium/.

asked Congress to pass new legislation.[23] Congress has considered a series of privacy and data security bills, but passed none. So the FTC began bringing enforcement actions against companies for failing to have "reasonable data security," initially premised on the theory that this was deceptive (given their data security promises)[24] and, by 2005, that this was unfair.[25] Unfairness had risen again, if timidly.

With the rise of a new guard of Commissioners, the FTC began to use its unfairness authorities more aggressively. In 2008, the FTC brought UMC and UAP claims against N-Data's alleged breach of pricing commitments for certain standard essential patents.[26] In 2009, new leadership at the FTC began pursuing unfairness cases more vigorously. The FTC brought a stand-alone Section 5 claim against Intel, which was settled early in 2010.[27] In July 2011, the FTC opened an investigation into Google's business practices that dragged into early 2013, with then FTC Chairman Jon Leibowitz publicly declaring his intention to use the Google case to revive Section 5 as an independent basis for UMC actions that the antitrust laws would not reach (because of substantive and procedural limitations imposed by the courts).[28] At the same time, the FTC used its UMC authority to secure consent decrees against Bosch and Motorola for their actions concerning standard essential patents.[29] Meanwhile, BCP began using unfairness to prosecute data security cases more aggressively,[30] as well as a number of other technology-related cases, including the design of software and hardware.[31] BCP has also used the bully

[23] Federal Trade Commission, *Privacy Online: Fair Information Practices In The Electronic Marketplace: A Report To Congress* (May 2000), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[24] Federal Trade Commission, *Eli Lilly Settles FTC Charges Concerning Security Breach*, Press Release (Jan. 18, 2002), http://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

[25] Federal Trade Commission, *BJ's Wholesale Club Settles FTC Charges*, Press Release (Jun. 16, 2005), http://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.

[26] Federal Trade Commission, *In the Matter of Negotiated Data Solutions LLC*, Press Release (Sept. 22, 2008), http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/09/negotiated-data-solutions-llc-matter.

[27] Federal Trade Commission, *FTC Settles Charges of Anticompetitive Conduct Against Intel*, Press Release (Aug. 4, 2010), http://www.ftc.gov/news-events/press-releases/2010/08/ftc-settles-charges-anticompetitive-conduct-against-intel.

[28] *See* Jon Leibowitz, *"Tales from the Crypt" Episodes '08 and '09: The Return of Section 5 ("Unfair Methods of Competition in Commerce are Hereby Declared Unlawful")*, Section 5 Workshop (Oct. 17, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/tales-crypt.episodes-08-and-09-return-section-5-unfair-methods-competition-commerce-are-hereby-declared-unlawful/081017section5.pdf ("all of us agree that there are circumstances in which the Commission ought to bring "pure" Section 5 cases.).

[29] *See* Federal Trade Commission, *FTC Order Restores Competition in U.S. Market for Equipment Used to Recharge Vehicle Air Conditioning Systems*, Press Release (Nov. 26, 2012), http://www.ftc.gov/news-events/press-releases/2012/11/ftc-order-restores-competition-us-market-equipment-used-recharge; Federal Trade Commission, *Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns*, Press Release (

[30] *See, e.g.*, Federal Trade Commission, *FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information*, Press Release (Jun. 26, 2012), http://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect; Federal Trade Commission, *FTC Filed Complaint Against LabMD for Failing to Protect Consumers' Privacy*, Press Release (Aug. 29, 2013), http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

[31] *See, e.g.*, Federal Trade Commission, *HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers*, Press Release (Feb. 22, 2013), http://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile; Federal Trade Commission,

pulpit aggressively to call on companies to adopt best practices, such as privacy and security "by design."

II. The Causes & Consequences of Excessive Discretion

Perhaps the central problem of today's FTC is the extent to which it takes advantage of its wide discretion to act, flowing from its broad statutory mandate and its institutional design. Among other things:

- The antitrust laws and Section 5 are (intentionally) vague, terse and amorphous.
- Even where the FTC itself has imposed limitations (through guidelines, rulemakings, and the like), its administrative enforcement process demands little specificity or consistency in its interpretation of these limits.
- In practice, the FTC often simply includes a perfunctory reference to limiting language in its administrative complaints, offering little content to flesh out its meaning or constrain the agency's discretion.
- Parties have little incentive to litigate in court to add definition to these terms, which leaves the Commission with considerable regulatory slack within which it can advance novel interpretations of Section 5 through consent decrees that go unchallenged.
- Other businesses (not parties to a consent agreement) lack any firm basis for understanding an agreement's terms and their significance, which magnifies the FTC's discretion to assert the boundaries of its own authority in future cases.

A. The FTC as an Institution

When we say that the FTC "has discretion" we really mean that the human decisionmakers at the Commission have discretion, as guided by their own judgment and that of those whom they may consult, and as constrained by any limitations imposed upon their decisions internally or externally.

1. Discretion of Individual Decisionmakers

One traditional approach to addressing concerns about an agency's discretion has been to commit that discretion to wiser decisionmakers. Indeed, this was the progressive-era genesis of the Commission: Congress, recognizing its own inability to put in place effective commercial regulation, created the FTC to exercise the expertise and flexibility to create the rules that it could not.

This approach, however, has serious drawbacks. Most important, it is limited by the ability to find irreproachable decisionmakers to helm the Commission – to steer unfailingly between Type 1 and Type 2 errors. For much of the Commission's recent history – since the difficulties of discretion the Commission faced in the 1970s into the 1980s – the Commission has been frequently lauded for its work.[32] Importantly, during this era the Commission's exercise of its power was implicitly constrained.

Peer-to-Peer File-Sharing Software Developer Settles FTC Charges, Press Release (Oct. 11, 2011), http://www.ftc.gov/news-events/press-releases/2011/10/peer-peer-file-sharing-software-developer-settles-ftc-charges.

[32] *See Financial Services and Products: The Role of the Federal Trade Commission in Protecting Consumers: Before the Senate Subcommittee on Consumer Protection, Product Safety, and Insurance*, 111th Cong. 10 (Mar. 17, 2010)

On the consumer protection side, it was constrained by the fresh institutional memory of the Congressional response to its excesses of the earlier era. And on the competition side, it was constrained by the still evolving economic antitrust consensus that had begun forming with Bork's THE ANTITRUST PARADOX.

More recently, the Commission has increasingly – and at times deliberately – shed these constraints. As documented elsewhere in this report, its work on the Consumer Protection side has taken an increasingly interventionist role, for instance in its data security and advertising cases. On the competition side, there is developing feeling that antitrust is too "pro-business," and the Commission unable to restrain perceived anticompetitive conduct relying on established antitrust principles. In response, commentators (including several Commissioners) have begun urging the FTC to make more aggressive use of its amorphous UMC authority instead of relying on that authority merely as a basis to enforce existing antitrust norms.

An important aspect of the Commission's recent efforts is that it has benefitted from the reputation it established over the prior 10-15 years. Having established itself as an extremely competent competition and consumer protection authority, it has commanded more respect (and discretion) as it has sought to expand its authority, even where its approach has changed significantly, such as in the area of standard essential patents.

2. Structural Discretion

The alternative to relying on decisionmakers to exercise constrained discretion is to rely instead on institutional design. This has the downside of imposing administrative costs: reducing agency flexibility and increasing the time required to make decisions. But it has the advantage of reducing the "human element" – and, in particular, reducing reliance on future, unknown, decisionmakers of uncertain discretion.

Structural restrains may be either internal (*e.g.*, internal agency procedures) or external (*e.g.*, judicial review of agency action). Perhaps the most important example of these constraints for the FTC are the rulemaking requirements imposed by Magnuson-Moss, which requires the FTC to engage in additional procedures beyond those traditionally required by the APA when engaging in rulemaking. These procedures are generally internal constraints, imposing additional requirements on the Commission's own decisionmaking process. But Magnuson-Moss also imposes external restraints, for instance by providing that rules must be provided to Congress for review before being enacted.

The basic premise of structural constraints on discretion is to open an agency's exercise of its authority to review by a larger number of decisionmakers. A basic example is the requirement that the FTC be helmed by a 5-member commission, of which a majority must approve any action. Fundamentally, this is not about constraining the power of the Commission – it's about constraining the discretion of

---

(statement of Timothy J. Muris, Foundation Professor, George Mason University School of Law), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=283c285e-53c8-4bf2-ad48-ee772b93d8c4 ("Given this impressive agenda and workload, in 2009 the Global Competition Review gave the FTC its highest rating out of 5 stars. The GCR stated that '[f]ew agencies in the world balance their antitrust and consumer protection duties as well as the U.S. Federal Trade Commission. While many agencies struggle to be good at one or the other, the FTC has mastered both.'") [hereinafter, "Muris Testimony"].

individual actors within the commission, to ensure that institutional decisions reflect a more learned, careful, and deliberative exercise of the Commission's discretion.

3. Sources of Restraint on Discretion

In principle, discretion at the FTC can be restrained, and guided, in a number of ways:

- Internal constraints & guidance
  - The very mentality that guides the agency may be the single greatest factor in understanding how it exercises its discretion, and depends largely on the identity and background of the Commissioners and, especially, of the Chairman.
  - Analytical rigor, such as in economics or technology, both disciplines which may help to predict unintended consequences and weigh costs.
  - Public statements of guidance or policy, which, at minimum, give rise to reputational constraints if such pronouncements are later ignored, and may provide basis for subsequent external constrains by the courts and Congress.
  - Checks and balances within the agency, such as from the Bureau of Economics ("BE"), a potential future Bureau or Office of Technology, and, vitally, Commissioners themselves.
- External constraints & guidance
  - The Courts, which may review agency decisionmaking for substantive and procedural compliance with the law.
  - Congress, which may exercise an enormous check on an agency through oversight and appropriations, even without substantively changing the limits of the agency's power or the legal standards or processes by which it operates.
  - The legal community, from much of which the agency's staff and commissioners are drawn and to which they will return.

B. The FTC as Administrative vs. Law Enforcement Agency

Assessing the appropriate balance between the FTC's distinct roles as an administrative and a law enforcement agency is fundamental to effective reform. Recent experience indicates that the FTC is operating more as an administrative agency exercising largely unfettered discretion than a law enforcement agency bound by the courts.

As an administrative agency, the FTC's primary form of regulation involves administrative application of a set of general principles – a "law enforcement" style function that, practically speaking, operates as administrative regulation for reasons described below. Although less frequent, the FTC also regulates through formal rulemaking. At the same time, the agency also engages as a law enforcement agency in litigation, invoking the processes and substantive rules of the courts to enforce and further interpret its regulations and the statutes it is charged with enforcing. Law shaped primarily, or at least ultimately, by the courts, is quite a different matter from regulation, in which the courts' involvement is episodic at best, especially regarding the law's substantive contours. Indeed, the more formal the regulation, the greater may be the courts' involvement. In some cases, such as mergers, the parties can often appease the regulators while achieving their business purposes without litigation. In other cases, a party must appear frequently before the same regulator and therefore has incentives to maintain good relationships. Meanwhile, in many cases, the agency seeks to retain its largely unfettered discretion and prefers to avoid judicially imposed limitations.

Despite the disadvantages of administrative regulation, in some areas it is the preferable process for addressing regulatory issues. All three processes – judicial, rulemaking, and administrative – are common throughout the administrative state, and at the FTC. The use of administrative processes rather than either rulemaking or judge made law is common elsewhere. The drug approval process is a prominent example of a hybrid process: Rules spell out an elaborate process, but the key substantive issues involve evaluation of the methods and results of clinical trials, in which the agency has enormous discretion with little judicial oversight.

The problem with administrative regulation is, as noted at the outset, the risk and cost of the excessive exercise of discretion by an agency unchecked by regular, if any, judicial oversight.

As an administrative agency, the Commission is delegated broad power. Consistent with its statute, it may make rules and regulations, conduct investigations, and adjudicate violations of its rules and regulations. This is all done under its own authority. There is some judicial (as well as Congressional) oversight of the agency's conduct – but what oversight there is occurs almost exclusively after the conclusion of the Commission's own process. And given the extent of the Commission's discretion, this infrequent oversight typically does not impose substantial limits on the agency.

Law enforcement agencies play a more limited – but no less important – role in the legal system. Like administrative agencies, they have substantial discretion over which investigations to conduct and which cases to bring. But the process of those investigations is more often (though not always) subject to judicial oversight. More importantly, law enforcement agencies bring enforcement actions in court, subject to the oversight of and adjudicated by actors that are independent of the agency (*i.e.*, Article III judges). A final, extremely important, difference is that law enforcement agencies do not have authority to make rules or regulations – that is, to say what the laws they enforce mean. Rather, the task of saying what the law means – and adhering to jurisprudential concepts such as *stare decisis* – falls to the courts.

While the FTC is known as a "law enforcement agency," in reality the FTC was deliberately structured to operate as an administrative agency and given the broad powers and discretion entailed. Indeed, this was done primarily so that the agency would have the flexibility to investigate and develop rules applicable to changing social and business norms. In 1914, there was concern that the Department of Justice and the courts, enforcing the antitrust laws, were unable (or unwilling) to keep apace of growing firms.

As one of the key legislative accomplishments of the progressive era, the discretion given to the FTC reflects the confidence of that time that sufficiently independent, accomplished and capable regulators could be trusted to use their discretion wisely to serve the public interest. The FTC was expected to apply that discretion in promulgating static rules that would bar conduct that harmed consumers and guide businesses on how to comply. It was expected, in other words, that the FTC would create (or help Congress to create) rules that would then be enforced in a law enforcement setting.

The modern administrative state as it has evolved over roughly the past 30 years (*e.g.*, since around the time of the Supreme Court's opinion in *Chevron*) recognizes agencies as operating more in the realm of policy than of law. Congress specifies the outer boundaries of an agency's "policy space," and the agency is free to specify – and to change – rules *within that space*. The latter part of that is important: agencies are generally free to change their established rules, so long as the new rules remain permissible under the agency's statute. In other words, *stare decisis* applies to court decisions but not to those of administrative agencies. Thus, while the Congress of 1914 intended to create an agency better suited than itself to establish a flexible but predictable and consistent body of law governing commercial

conduct, the modern trend of administrative law has relaxed the requirement that an agency's output be predictable or consistent.

The FTC has embraced this flexibility as few other agencies have. Particularly in its efforts to keep pace with changing technology, the FTC has embraced its role as an administrative agency, and frequently sought to untether itself from ordinary principles of jurisprudence (let alone judicial review). In its privacy and data security cases, for example, the Commission has used its administrative process to extract an expansive, and increasingly ad-hoc, series of consent decrees from firms. These consent decrees are reached using a one-sided investigation process, backed by the threat of potentially embarrassing and expensive administrative adjudication. None of this is reviewed by the courts. As a result, these consent decrees contribute little to the development of a stable or predictable body of law. Similarly, in its UMC enforcement, the Commission has sought to untether aspects of its competition authority from the constraints of traditional antitrust law; rather, it would prefer to operate under a discretionary standard, where it – not the courts – both decides what the law means and adjudicates violations of it. Given that the courts rejected the FTC's most recent litigations on UMC and have yet to test the FTC's approach to privacy and data security cases, the FTC's actions have been unmoored from judicial oversight.

The predicates for this power and approach are not unreasonable. There is legitimate need for an expert agency with the flexibility necessary to develop efficient and predictable rules in a changing environment. But the FTC has occasionally gone quite far to the administrative extreme, and greater judicial oversight may be needed to ensure that the agency's work actually benefits the consumers it is meant to protect. Even within the realm of enforcement, some have adduced evidence to suggest that the FTC's subject-matter expertise improves little upon generalist courts.[33] So is it time for a rebalancing of the Commission's roles as an administrative versus law enforcement agency? If so, how?

C. The Challenges Created by Technology

Technological change presents regulatory challenges precisely because it is disruptive (or, perhaps, it is disruptive technology that presents regulatory challenges). The term "disruptive" is a term of art, albeit one that acquired mythological or religious quality. But from a legal perspective, "disruptive" means that a new technology alters (or appears to alter) the antecedents upon which current legal rules are based – *that*, rather than existing business models or market shares, is the key thing which such technology disrupts.

These changes in the underlying assumptions of a legal regime are problematic for several reasons. First, they create an exigent demand for new rules as both those who benefited under the prior rules and those disadvantaged by the technology will seek regulatory restrictions upon new technology. Second, by its very nature (*i.e.*, the circumstances of the prior legal rules having changed), would-be regulators operate in an uncertain legal environment. Third, and especially in the modern setting, the pace of change can be very rapid. Fourth, because the sources of these changes are hard to predict, regulators seek (and are often given) broad, flexible powers and substantial discretion to address them. And fifth, but far from least important, such regulation is often a reflexive response, one that preserves the prior regulatory regime (and benefits its entrenched interests) without weighing the consumer benefits of the

[33] *See* Joshua D. Wright & Angela M. Diveley, *Do Expert Agencies Outperform Generalist Judges? Some Preliminary Evidence From The Federal Trade Commission*, 1 J. ANTITRUST ENFORCEMENT 82 (2013).

new and old regimes. The current ongoing battle between taxi regulators and services like Uber exemplify these trends, as regulators (spurred on by incumbents) rush in to regulate these services without an understanding of their benefits.

These concerns can be summarized succinctly: there is great pressure for regulators to "do something" in response to new technology, but it is usually unclear what that "something" is or whether it will benefit consumers. Importantly, the concept of "new technology" isn't restricted to technology-related businesses. These same concerns arise as firms in any industry incorporate new technology into existing businesses, or as new business techniques give rise to new business models. A firm need not be doing technology-related work for innovation to disrupt some aspects of its business.

Unfortunately, in the rush to do something, the fact that doing the wrong thing can be harmful is often lost. The history of regulation is replete with examples of failed regulation – the most egregious of which are cases where regulatory efforts have in fact created anticompetitive conduct or otherwise *caused* substantial harm. The best-case scenario for regulation is often where the regulatory regime proves to be irrelevant.

There is a strong practical argument against the notion that the FTC, or any government agency, should attempt to develop explicit technology based standards: Such standards would quickly become obsolete, given the constantly shifting nature of technology. Clearly, no regulatory agency can adapt quickly enough to keep such rules current. As the Unfairness Policy Statement put it: "[Section 5] was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[34] On the other hand, delineating general rules for specific technologies risks deterring technological experimentation and innovation and slowing technological advance.

These issues – the pressure to do something, the uncertainty as to what that something is, and the potential for that something to in fact be harmful – give rise to a set of competing concerns for how agencies such as the FTC operate. On the one hand, regulators need the ability to act flexibly and quickly if they are to have relevance in rapidly changing settings, and Congress may need to delegate broad power and substantial discretion to them (because Congress cannot know, *ex ante*, what challenges new technologies may bring). There is even an argument for intervening *earlier* in high-tech markets, rooted in the error cost framework but built on the assumption that the costs of *not* intervening, even in the face of uncertainty, are higher than the costs of erroneous intervention.[35]

On the other hand, the risk that unwise regulation can wreak havoc upon regulated industries cautions restraint and humility, and a reluctance to use any broad powers or discretion (because, like Congress, even the FTC cannot know, *ex ante*, how technology will continue to evolve).

[34] Unfairness Statement, *supra* note 1.

[35] *See, e.g.*, TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2010).

III. Institutional & Process Issues

A. Discretion Generally

Efforts to address the extent of the Commission's discretion must assess the trade-off between too much and too little flexibility. The central questions relating to discretion concern how much the FTC needs in order to carry out its mission, how much it actually has today (in the exercise of each of its various authorities), and how specifically to constrain the Commission's use of its discretion where it is nevertheless needed. This last consideration is paramount, because it is not possible to perfectly fit the extent of the agency's discretion to its mission – invariably it must have more power than is minimally necessary in order to carry out its mission.

With this in mind, the following questions are important to any discussion of FTC discretion:

- How much discretion does the Commission have in different areas (*e.g.*, UDAP vs. UMC)? How does it vary based upon how the Commission acts (*e.g.*, if it proceeds first through an ALJ in its enforcement actions)?
- In what way may the Commission's exercise of its discretion be constrained?
    - Should Congress narrow the agency's substantive authority or jurisdiction, either in general or in specific areas?
    - Should Congress constrain the agency's investigative powers (*e.g.*, its ability to issue CIDs)? If so, how to do this without limiting the Commission's ability to conduct investigations (*e.g.*, *ex ante* vs. *ex post* review of CIDs)?
    - Should procedural safeguards on the agency's use of its power be implemented, either as a matter of agency practice or through legislation (*e.g.*, should a Competitive Impact Statement be required to accompany any administrative adjudication or rulemaking)?
- Can the FTC increase internal institutional safeguards (*e.g.*, by requiring separate approval of the Bureau of Economics, and/or the office of the Chief Technology Officer, prior to undertaking any administrative or investigative action)?
- How might Congress increase external institutional safeguards, particularly from the courts?
    - Currently judicial approval is required for merger injunctions and other equitable relief such as disgorgement. Should other substantive agency decisions require similar judicial review?
    - How much deference (*e.g.*, *Chevron* deference) does the Commission receive when exercising its various authorities?
- How do we respond where the Commission seeks to increase its authority beyond historically recognized norms, for example:
    - The Commission's desire to untether UMC from the traditional antitrust laws?
    - The Commission's use of a "common-law-of-settlements" in developing data privacy law?
    - The Commission's application of all existing requirements to bring an action under Section 5 and/or its policy statements (or lack thereof)?
    - The Commission's desire for increased powers in fraud cases (especially in seeking damages and for third-part liability)?
    - The Commission's increased activity, under broader standards, for advertising claims?

- With the Commission's increased activity against companies that allegedly "assist" fraudsters,[36] is the agency trying to claim powers Congress declined to give it in 2010?
- What are the agency's enforcement powers, generally and vis-a-vis DOJ, CFPB, etc.?

B. Rulemaking & Guidance

1. Rulemaking

Again, after the FTC began its rulemaking spree, Congress created a formal rulemaking process for the agency under Section 5 in the 1975 Magnuson-Moss Act and imposed additional procedural safeguards in its 1980 amendments to Magnuson-Moss. That formal rulemaking process has since gone unused (for new rulemakings). Instead, Congress has passed specific pieces of legislation requiring the FTC to undertake a rulemaking regarding issues that could, at least arguably, have been addressed through a Magnuson-Moss rulemaking, like the Do-Not Call registry.[37] Moreover, the Commission has succeeded in crafting informal rules through its adjudicatory process. Where that litigation has evolved entirely or largely by settlement the FTC has been able to shape law without the discipline required either by Magnuson-Moss or by normal judicial scrutiny.

In general, the FTC has essentially refused to use the Magnuson-Moss process. The Commission's most recent former Chairman, Jon Leibowitz, routinely insisted that Magnuson-Moss was "medieval," and he lobbied aggressively to abolish the Act and to give the FTC the ability to make formal regulations through the Administrative Procedures Act typically used by regulatory agencies (and which the FTC itself uses in certain areas where Congress has given it specific statutory authority.

- Do the concerns that animated Congress' decision to enact Magnuson-Moss still pertain today? In other words, are consumer interests better served by the FTC enacting rules under broader (APA) or narrower (Magnuson-Moss) constraints? Or would the problems with the FTC's use of its discretion simply be compounded?
- Whether a result of the perceived need to sidestep Magnuson-Moss or not, is there nevertheless value in incentivizing Congress to influence the agency's rulemaking agenda by passing legislation in specific areas (*e.g.*, Do Not Call)?
- What is the scope of the FTC's UMC rulemaking authority under Section 6(g)?[38] What procedures are required for it to use this authority? When has it used this authority in the past?
- Why hasn't the FTC used its Magnuson-Moss rulemaking power? Is it really as burdensome or difficult as some FTC Commissioners have insisted? Or is it simply unnecessary given the FTC's ability to make rules through adjudications without effective restraint?

[36] *See, e.g.*, Federal Trade Commission, *FTC Sues Payment Processor for Assisting Credit Card Debt Relief Program*, Press Release (Jun. 5, 2013), http://www.ftc.gov/news-events/press-releases/2013/06/ftc-sues-payment-processor-assisting-credit-card-debt-relief-scam.

[37] *See* Muris Testimony, *supra* note 32, at 22-29.

[38] *See* Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, § II.B.1.b, http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last revised July 2008).

- Are there areas where Magnuson-Moss could be used effectively today, and might provide clearer guidance to industry? For example, could the FTC use this rulemaking authority to achieve a national data breach notification standard?
- Could Magnuson-Moss be made easier or faster to use without changing the substantive standards for rulemaking or removing key procedural safeguards?

2. Guidelines & Policy Statements

Among the agency's activities, the issuing of guidelines, policy statements, advisory letters and the like regarding its own authority are unique in that they tend to *restrain* the scope of the agency's discretion rather than expand it. Other than increased judicial oversight (or legislated jurisdictional limitations), self-imposed guidance may be the most effective procedural tool for cabining agency discretion.

Ideally, the agency's guidelines and policy statements are constituted to accurately reflect agency practice and legal interpretations, offering insight into the agency's decision-making process, the benefits of its expertise and a clear signal of its likely future actions. Because guidelines are not binding, actual enforcement (and regulatory) actions may deviate from their prescriptions. However, guidelines and other policy statements may have important effect on subsequent agency actions. For instance, they may affect a court's subsequent evaluation of an agency action, or provide potential litigants with insights needed to mount an effective judicial challenge. Should the agency act contrary to its published position, this may provide impetus for Congressional scrutiny of the agency. And, at minimum, deviation from its prior published statements may incur reputational harms of concern to the Commission.

Despite (or because of) their imposition of constraints on discretion, some of the FTC's guidelines have been enormously successful. The Horizontal Merger Guidelines (HMGs) have historically "provide[d] a flexible, comprehensive, and administrable approach," while still remaining both "broadly applicable and providing certainty to businesses and practitioners."[39] Moreover, they seem, generally, to reflect actual agency practice. That said, it is telling to note that the FTC and DOJ's decision to revise these guidelines in 2010 has been met with criticism – it remains to be seen how they will be embraced by the courts and what lasting effects they will have on merger review.

- What is the legal impact of different statements of guidelines and policy? In what ways are they formally binding upon the agency? What level, if any, of deference do they receive from the courts?
- Under what circumstances is it appropriate for the Commission either to, or not to, issue such guidance? Should the Commission provide guidance?
- What informal constraints do guidelines, policy statements, and the like place upon the agency? What are the mechanisms of these constraints?
- To what extent has the FTC been bound by such documents in the past? To what extent has the commission altered, or otherwise declined to follow, such guidance in the past?
- To what extent are those subject to such guidelines influenced by, or do they otherwise rely upon, them?

[39] Timothy J. Muris and Bilal Sayyed, *Three Key Principles for Revising the Horizontal Merger Guidelines*, ANTITRUST SOURCE 3-4 (April 2010), *available at* http://www.law.gmu.edu/assets/files/publications/working_papers/1256ThreeKeyPrinciples.pdf.

- To what extent do those with authority over the agency rely upon such guidelines and policy statements in evaluating the performance or decisions of the agency?
- To what extent does the ease with which the Commission can revoke guidance *(e.g.*, the revocation of the Disgorgement Policy Statement without any public comment or other process beyond a vote of the Commissioner diminish the value of whatever guidance the Commission does provide? Can the FTC actually become more effective in steering industry if it binds its future discretion by making it more difficult to revoke guidance once given?
- What is the proper role of highly informal guidance like Frequently Asked Questions? For example, was it appropriate for the FTC to conclude its revision to the Children's Online Privacy Protection Act ("COPPA") rule while assuring industry that some of their concerns would be addressed in FAQs? Are these FAQs really new regulations and should the FTC, in such situations, issue further Notices of Proposed Rulemaking?

C. Information Gathering

1. Section 6(b) Investigations

Section 6(b) of the FTC Act gives the Commission the authority "to conduct wide-ranging economic studies that do not have a specific law enforcement purpose" and to require the filing of "annual or special … reports or answers in writing to specific questions" for the purpose of obtaining information about "the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals" of any company over which the FTC has jurisdiction, except insurance companies. This section is a useful tool for better understanding business practices, particularly those undergoing rapid technological change.

- But the costs of these investigations can be significant, both to the FTC and to companies. How should the FTC weigh these costs? Should the Paperwork Reduction Act be amended?
- Is the FTC making full use of the information it already has? It is adequately equipped to do so?
- What principles, if any, should limit the FTC's discretion in conducting 6(b) inquiries?
- Has the FTC attempted to use 6(b) orders to shape business practices, by focusing attention on certain practices and using the Commission's bully pulpit to call for change? For instance, the Commission's ongoing inquiry into "data brokers"[40] has been targeted so broadly as to redefine that term to include many companies that never considered themselves "data brokers" (a term with increasingly negative connotations), while one Commissioner has pressed industry hard for greater transparency around the uses of consumer data through the appealing brand of "Reclaim Your Name." Is this an appropriate use of Section 6(b) – or the FTC's bully pulpit?
- Conversely, should Section 6(b) continue to bar the Commission from gathering information about insurance companies without specific Congressional authorization to do so?

[40] Federal Trade Commission, *FTC to Study Data Broker Industry's Collection and Use of Consumer Data*, Press Release (Dec. 18, 2012), http://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data.

2. Omnibus Resolutions

In competition cases, the entire Commission must vote to authorize CIDs in each matter and also vote to close investigations once compulsory process is issued. But in consumer protection investigations, there are standing Commission orders authorizing compulsory process for certain types of investigations. For instance, there is a standing Commission order authorizing staff to investigate telemarketing fraud cases. Thus, if staff wants to issue a CID to investigate a certain telemarketer, it need only seek approval of the CID from the Commissioner assigned that matter (much like a judge assigned to "sit circuit"). In such cases, the other Commissioners do not have an opportunity to vote on the issuance of the CID and would not know about the investigation. The Chairwoman effectively controls the staff, by virtue of appointing the senior staff, and thus can control setting the agenda of agency staff. Thus, because of omnibus resolutions, some cases not presented to the other Commissioners to determine whether the investigation is an appropriate use of the agency's resources or whether the legal basis for the case is sound, and in some cases, the other Commissioners may not even see the case until a settlement has been negotiated as a *fait accompli*. Since the Chairman's office can always assign a matter to itself, the most important and sensitive matters may be handled by the entirely by the Chairman.

- Are omnibus resolutions legal under the FTC Act?
- How large a problem is this? To what extent has the omnibus resolution process diminished the ability of Commissioners to oversee the work of agency staff, to check the discretion of the Chairman, and, in particular, of minority Commissioners to provide an effective alternative to the approach of the majority?
- Which, if any, omnibus resolutions should be retained? Why? How valuable are they as an administrative convenience in expediting run-of-the-mill UDAP investigations? How should the Commission decide when those benefits outweigh the costs to transparency within the agency?
- If omnibus resolutions are retained, can the process be modified to ensure that they are not abused?

3. HSR Premerger Notification Disclosures

The Hart-Scott-Rodino (HSR) Antitrust Improvements Act requires firms engaging in mergers or acquisitions above certain size thresholds to report these transactions to the FTC (and DOJ; one of the agencies will be assigned to review each transaction) at least 30 days prior to the transaction's closing. The purpose of this is to allow the agencies to challenge potentially anticompetitive transactions prior to closing, on the grounds that after a transaction closes it may become very difficult to "unscramble the eggs" should the transaction prove to have anticompetitive consequences.

Should the reviewing agency determine that a transaction may be problematic, it can submit a "Second Request" for information from the parties to the transaction. This is effectively a subpoena for information. The transaction then cannot proceed until the parties have complied with the Second Request and the reviewing agency has had at least an additional 30 days to review the transaction. The information requested in a Second Request is often voluminous, can impose substantial costs (both in terms of time, money, and resources) to collect, and can take many months for the parties to provide, further delaying a transaction.

In addition, the basis of the HSR process is to allow the reviewing agency to make informed predictions about the likely outcomes of a given transaction. That is: to determine whether the transaction is likely to substantially lessen competition. This can be a difficult, if not impossible task – and it is one that often

leads to particularly burdensome Second Requests, as the agency attempts to make judgments about myriad dynamic, and often nascent, industries.

- How much information should the FTC be able to demand as part of the Second Request process? Historically, it has agreed to self-imposed restraints, such as the number of custodians parties must provide documents from, or search terms parties must use. Are these sufficient? What is the legal basis for such restraints?
- An important metric for the agency is it's "win rate" – that is, the number of cases that it wins versus the number of cases that it brings. How does this affect its review of mergers, where the "win" for consumers is often to allow a transaction to proceed?
- How long should this process take? What are the costs that this process imposes upon firms?
- How should merger review proceed in dynamic industries? What is the role of nascent or developing markets in merger evaluation?
- What forms of evidence are appropriate to consider in blocking a transaction, and what weight should they have? For instance, how should economic data and models that do not support challenging a transaction be weighed against business documents (so-called "hot docs") containing statements that indicate anticompetitive hopes for the transaction (e.g., "This transaction will allow us to corner the market on widgets and raise prices 80%!)"
- What protections do, or should, exist for third parties subject to CIDs for information relevant to a merger?

4. Civil Investigative Demands (CIDs)

To the extent that the tendency of companies to settle FTC enforcement actions out of court explains why the courts have been involved so little in the development of Section 5, much of the reason for that tendency may lie in the application of Section 20, which allows the FTC to issue Civil Investigative Demand (CID) orders instead of having to get a federal court to issue subpoenas, as normal plaintiffs must do.

- Are the FTC's CIDs too broad? Is BE adequately assessing CIDs before issuance?
- How costly are CIDs? Could BE perform a study on these costs, and how they affect settlement negotiations?
- Has the FTC used overly broad and duplicative CIDs to raise the costs to companies of not settling?

D. Enforcement

1. Case Selection

Given the FTC's nature as a law enforcement agency, and its success in settling cases in a manner that approaches regulation as described above, how it selects the cases it brings may be the most important aspect of its discretion.

- In deciding whether to open an investigation or bring an enforcement action, how does the FTC apply its "Reason to Believe" standard, assess whether the case is worth the agency's resources, and whether it is in the public interests?
- What consideration does the agency give to likely remedies, potential unintended consequences, and error costs?

- How well, and how, foes the FTC guard itself against being used as merely a tool in battles among competitors, especially by those who are seeking to stop innovative disruptive technologies, to the detriment of consumer welfare?

2. Part III vs. Article III Adjudication

There are important differences between adjudications that proceed initially in administrative (e.g., Part III) vs. judicial (e.g., Article III) venues. In some cases, the FTC is required to proceed initially in one venue or the other; on other cases, it may have a choice in which venue to initially proceed (which it may use to its strategic advantage). The selection of venue can affect the FTC's likelihood of success, the deference it will receive from courts, the costs imposed upon litigants (and therefore their willingness to settle), the range of discovery options available, the range and sort of materials considered by the tribunal (e.g., through amicus briefs), the extent to which the tribunal's decision creates norms or rules binding upon other parties, and the extent to which those parties receive notice about or have opportunity to challenge those rules.

These concerns give rise to myriad questions about the availability of administrative vs. judicial adjudication to the FTC, which is the proper venue for the Commission's various enforcement actions and the power of the Commission in some cases to select its initial forum.

- What is the current scope of the FTC's authority to litigate in federal courts independent of the Department of Justice? Should that authority be expanded?
- Should the FTC retain the ability to bring all enforcement actions through its Part III administrative process? Should the FTC instead always have to litigate in federal court? If administrative costs are the main reason for retaining Part III, could Part III become essentially a small claims court to allow the FTC to prosecute certain cases without the expense of Article III litigation?
- What kind of deference might the FTC receive in interpretations of Section 5, depending on what kind of action it takes (*e.g.*, *Chevron*)? Should that deference be altered by Congress?
- How does the Commission's decision of how to proceed affect its ability to "win" cases? How does it affect the availability of discover to the Commission – and the costs of discovery upon litigants and third parties? How does the requirement that litigants appeal through the Commission to final agency action before being heard in an Article III court affect outcomes?
- How do outcomes of Part III vs. Article III adjudication differ in terms of how they establish rule-like legal norms (*e.g.*, in terms of the correctness of these rules, the range of factors they consider (from other industry actors, affected parties and other sources), and the information and notice they provide to other parties about the future applicability of these rules?

3. Negotiation of Consent Decrees

Central to understanding the FTC's current discretion, especially in unfairness cases, is the question: Why do companies so often settle FTC enforcement actions? Understanding this question requires answering a host of more complicated questions:

- What drives the overwhelming tendency to settle enforcement actions? Is that tendency actually significantly greater with respect to the FTC than with respect to other agencies?
- Why does the tendency to settle vary, if it does, between DAP, UAP, UMC and antitrust actions? Do these differences reflect differences in the degree of doctrinal development or varying substantive standards, or something else?

- To what extent does the expense and nature of the FTC's CID process drive companies to settle cases they might otherwise litigate? Could targeted reforms to that process encourage sufficient litigation to sufficiently constrain the FTC's discretion in bringing future enforcement actions?
- How large a causal factor is the FTC's ability to force a defendant unwilling to settle to go through the Part III administrative adjudication process before getting to an Article III court? Would reforming, or partially eliminating, Part III litigation help?
- Or does the tendency towards settlement stem more from the public relations consequences of challenging the FTC, particularly on issues like data security and privacy? If so, is the FTC's use of its bully pulpit appropriate?
- Is there anything improper or harmful about the practice of FTC staff conducting investigation with a standardized "pocket settlement" in hand? Does this create improper coercion or inadequate tailoring of remedies to the facts of each case?
- Do Commissioners have adequate opportunity to oversee the process by which consent decrees are negotiated?
- How does the Commission weigh error costs as it charts the direction of the law through negotiating consent decrees?
- In which forum should the agency proceed when seeking preliminary injunctions, especially of mergers (*e.g.*, where it enforces the same laws as the DOJ, but has available the option of administrative adjudication that the DOJ does not)?
- Should litigants be able to appeal directly to an Article III court without waiting for final agency action, or otherwise influence the initial choice of venue?

4. Enforcement of Consent Decrees

In some areas of law, the FTC operates entirely by settling enforcement actions in consent decrees, most notably data security. Consent decrees, generally with 20-year terms, are also increasingly becoming a tool for informal policymaking, allowing the Commission to require individual companies to require things that are not required by law and thus might more appropriately be addressed on a general basis through the rulemaking process. This is particularly true in the high-tech sector and on issues such as privacy. With nearly every major large technology company operating under a consent decree, many have asked whether the FTC is moving towards a form of regulation in which its discretion will be even more unconstrained, as companies face additional pressure to settle alleged violations of consent decrees because they face monetary penalties (unavailable in Section 5 cases) and even worse public relations fall-out than for violations of Section 5.

- What limits should there be on the FTC's discretion in setting the terms of consent decrees? How far may the Commission using consent decrees to make policy, such as by requiring "privacy by design" or "security by design?" Is the FTC improperly using consent decrees to effectively regulate particular companies, or entirely industry sectors?
- Is the FTC rigorously fulfilling all requirements for UDAP under Section 5 and/or its policy statements in bringing consent decrees (*e.g.*, properly finding materiality when claiming that privacy policies are deceptive)? If not, what type of internal or external oversight would be needed to ensure that it does so?
- How should the FTC distinguish between violations of a consent decree and independent violations of Section 5? In other words, how closely related must new conduct be to be considered a direct violation of the consent decree?

- Are the standards for determining whether a company has violated a consent decree different from those of establishing a Section 5 violation? Should the FTC be allowed to create consent decree requirements that are unmoored from the requirements of Section 5 or the Unfairness and Deception policy statements?
- Are 20-year consent decrees too long? Is the FTC enforcing consent decrees consistently, or are different officials interpreting these decrees in inconsistent ways?
- How should monetary penalties for consent decree violations be calculated?
- If a company has agreed to a consent decree based on legal theories that are invalidated by a future court decision, legislation, or other FTC action, or if a provision in a consent decree is later similarly invalidated or called into question, what process is there for having that provision nullified? If there is not one, should there be?

5. Consent Decrees as Guidance

In cases where the agency does act, complaints describe numerous potential problems but few insights into which ones were particularly important to the decision to proceed. For example, the desire to avoid suggesting that any one step is the key to information security has trumped the need for guidance to the regulated community about what is important and what is not. Such lack of guidance could well violate judicial requirements that agencies must, to satisfy constitutional standards of due process, provide "fair notice" of their policies, although that judicial doctrine may be underdeveloped. What particularly merits investigation, however, is whether a different standard should apply in the case of data security and merger guidance, and what the consumer welfare consequences of this divergence are.

In many instances consent agreements are efficient and effective. However, such agreements have a number of problems that certain reforms could mitigate. For example, the FTC could issue competitive impact statements with each settlement, including a fuller discussion of the agency's reasoning, the importance of particular facts and legal arguments, and clarification of general principles

6. Due Process & Fair Notice concerns

Three key questions are currently pending in litigation:

- Has the FTC's approach to data security provided adequate guidance to ensure fair notice?
- At what stage of litigation should due process concerns be raised?
- What should be the FTC's pleading burden in UDAP cases?

a) Fair Notice

Wyndham has asked the federal district court to dismiss the FTC's claim that the company's failure to provide "reasonable" data security constitutes an unfair trade practice because the FTC has failed to provide "fair notice" as to what would constitute reasonable data security. Wyndham relies on the Supreme Court's decision in *FCC v. Fox* (2012).[41]

[41] After the FCC changed policy regarding the utterance of expletives and glimpses of nudity during daytime TV, the Court held that broadcasters had a constitutional right to be warned in advance of what the FCC's new policy against indecency prohibited.

- To the extent that the FTC has prosecuted companies for having unreasonable data security for failing to follow data security practices recommended by the Safeguards Rule or that are actually industry best practices, has the FTC really failed to provide fair notice?
- More generally, what would constitute "fair notice" as to what Section 5 requires? Is the point of the doctrine requiring notice as to the right "standards" in a particular area or rather how the core elements of unfairness – substantial injury, countervailing benefit and reasonable avoidability by consumers – are weighed against each other?

b) When Must Fair Notice Questions Be Resolved?

The Wyndham litigation currently hinges on the question of how early in the litigation process questions of fair notice may be addressed. At a procedural level, the question has important implications for the *Wyndham* case, insofar as it may control whether fair notice claims can be heard at the Motion to Dismiss phase or, instead, must be heard following discovery at the summary judgment or trial stage. Perhaps more important, the question affects whether fair notice, especially as a Constitutional Due Process issue, places a burden upon the FTC to ensure that those subject to its regulations are reasonably appraised of them, or whether the burden is instead upon regulated parties either to be aware of the Commission's rules or to prove the negative facts that they were both reasonably informed but nonetheless unaware for the Commission's intended legal standard.

- If fair notice claims cannot be resolved until a motion for summary judgment, what effect will this have on defendants' willingness to litigate? Conversely, will such a rule further increase the tendency of companies to settle enforcement actions with the FTC and thus reduce the likelihood that courts will play a role in limiting the FTC's discretion in interpreting the boundaries of Section 5?
- Absent a clear judicial ruling that fair notice claims must be resolved at the MTD stage, could the FTC commit to resolving such questions at the MTD in, for example, an Enforcement Policy Statement? What are the practical arguments for and against such a policy? Should Congress legislate such a requirement?
- How should fair notice (and other Constitutional) claims be handled in Part III administrative litigation? Should the same arguments for resolving fair notice claims at the MTD stage should not apply equally, or even more strongly, in Part III matters? Have the Commission and its ALJ given appropriate consideration to Constitutional concerns raised by defendants?

c) What Should Be the FTC's Pleading Burden in UDAP Cases?

More generally, how much factual support and legal analysis must the FTC offer in its complaints to explain what constitutes alleged deception or unfair practice? Wyndham – supported by an amicus brief signed by several members of this Project[42] – has asked the district court to dismiss the FTC's complaint for failing to plead enough facts to make the FTC's claims more than "threadbare conclusions of law."[43]

[42] *See* Brief of Amici Curiae TechFreedom, International Center for Law & Economics, & Consumer Protection Scholars, FTC v. Wyndham Worldwide Corp., 2:13-cv-01887-ES-SCM (2012), *available at* http://bit.ly/1j9IKEo.

[43] Under the Supreme Court's decisions in *Twombly* and *Iqbal*, plaintiffs, including the government, must plead enough factual material to make out a plausible basis for relief. Further, Federal Rule of Civil Procedure 9(b)

At most, the FTC may need to amend or re-file its complaint against Wyndham, yet the question could fundamentally change how the FTC builds law under Section 5 in two respects: making companies more likely to litigate (thus producing fewer settlements and more judicial decisions), and making settled cases more useful as guidance. The questions raised here parallel those above regarding fair notice:

- As a legal matter, what pleading requirements is the FTC subject to? How long might it take to get a clear court decision?
- As a policy matter, should the FTC voluntarily commit to heightened pleading requirements, such as in an Enforcement Policy Statement? Specifically, Should the FTC more fully plead certain allegations, such as UAP's requirement of substantial injury and DAP's requirement of materiality? Or should Congress legislate such pleading requirements, as it has done for other "Special Pleading Matters" under FCRP Rule 9?
- Is there any reason why the same requirements should not apply equally in Article III litigation and Part III administrative litigation?
- What are the arguments for and against such requirements? Would they hamper the FTC's enforcement actions? Or is the FTC in a unique situation because, unlike normal plaintiffs, it can conduct generally significant discovery through its CID process, and thus should be able to draft complaints with greater particularity before proceeding in normal litigation? Conversely, what about fraud cases, where the agency's first direct contact with the defendant is its attempt to seek a temporary restraining order to block immediate further consumer injury?

E. Competition Advocacy

Antitrust law coexists with countless regulatory programs at the federal, state, and local levels that, intentionally or not, often restrict entry and limit output. Regulatory schemes often straitjacket competitive forces that, if unleashed, would improve economic performance and consumer welfare.

The FTC occupies a unique position in its role as the *government's* competition scold. Despite the absence of direct legal authority over government actors (which limits the efficacy of competition advocacy efforts), some have argued that "the commitment of significant Commission resources to advocacy is nonetheless warranted by the past contributions of competition authorities to the reevaluation of regulatory barriers to rivalry, and by the magnitude and durability of anticompetitive effects caused by public restraints on competition."[44] Most recently, the FTC has recently received broad acclaim for comments it has filed opposing efforts by taxicab commissions to block entry by Internet-based alternatives to traditional cab services, like Uber and Lyft.

There is generally broad support (at least outside of government) for the FTC's competition advocacy role. Indeed, if there is a consensus, even among those critical of other aspects of the FTC's approach, it is for the FTC to do *more* competition advocacy.

---

requires heightened pleading when a plaintiff alleges "fraud," which, Wyndham argues, includes Section 5 deception claims. In such cases, a plaintiff must allege the factual basis of the cause of action with particularity. The FTC insists 9(b) does not apply but argues, nonetheless, that it has satisfied the requirement if it does apply.

[44] Gellhorn, & Kovacic, *supra* note 6.

- How can the Commission bolster its competition advocacy efforts? Should competition advocacy take greater priority in the agency's budget requests relative to enforcement and other functions?
- How should the FTC prioritize its competition advocacy efforts?
- Do barriers to technologically disruptive companies like Uber deserve greater emphasis?
- How should competition advocacy relate to, and support, broader policy objectives? For example, given the emphasis placed in the FCC's National Broadband Plan (a report commissioned by Congress on promoting broadband investment, deployment and competition), should the FTC use its competition advocacy tools to attempt to reduce regulatory barriers to the deployment of broadband infrastructure?
- Should Congress get involved? Can Congressional hearings and letters help to amplify the FTC's competition advocacy efforts by calling attention to anti-competitive barriers to entry, especially regarding new technologies?

F. Institutional Structure

1. The Role of the Bureau of Economics

Implementing more and better economic analysis at the FTC should begin with a consideration of how the agency can make better use of the considerable economic expertise in its Bureau of Economics. The FTC is an unusual agency in that it has a large staff of economists; it should leverage that capacity. In particular this expertise must be applied in a meaningful way in consumer protection issues.

Relatedly, benefit-cost analysis should be more widely used by the agency. For example, ongoing privacy discussions have been largely devoid of any rigorous benefit-cost analysis. This should be rectified, and institutional reforms put in place to ensure that benefit-cost analysis is both rigorous and a meaningful check on agency discretion.

The Bureau of Economics has long shaped the Bureau of Competition's implementation of the antitrust laws, both by having a formal role in competition enforcement and by having a leading role in writing the antitrust guidelines co-authored by the FTC and Department of Justice. But what is BE's role in consumer protection matters, and what *should* it be? Indeed, what is the role of economics as a discipline in limiting the FTC's broad discretion to define UDAP, and in ensuring that the FTC's UDAP efforts do not inadvertently harm competition? Specifically:

- As discussed below, the FTC increasingly uses its deception authority beyond enforcement of traditional marketing claims to enforce codes of conduct, FAQs, help files and other informal statements, it is testing the presumption of materiality that once made sense to ensuring that consumers got the benefit of the bargain promised then. What is the role of economics, and the BE, in shaping the emerging, expanded doctrine of materiality? Would there be any basis for no longer using materiality to determine whether consumers have been harmed by the targeted conduct?
- The Unfairness Policy Statement clearly defines consumer injury as the lodestar of Section 5 and demands cost-benefit analysis by requiring that the FTC weigh injury against countervailing benefits to consumers or to competition. Yet, with scant litigation of unfairness cases, both UAP and UMC, how much cost-benefit analysis has the FTC really engaged in in practice? What has been the BE's role in this process? What should it be?

- Indeed, why should the BE's role in selecting cases for enforcement and defining the appropriate legal arguments differ between competition and consumer protection cases? Is it simply a question of volume and scale?
- What role has economics played in informing the FTC's policymaking function? In particular, the FTC has produced a series of reports and conducted a number of workshops regarding consumer privacy. Have these been appropriately informed by economics?
- Where the FTC has engaged in rulemakings, *e.g.*, in revising the COPPA Rule, has the FTC given adequate consideration to the economic consequences and trade-offs of its proposed revisions?
- Does the current regulatory impact process effectively assess the impact of regulation on innovation? Are compliance costs really what matters in sectors driven by small businesses, especially startups, or can even relatively small compliance costs discourage investment from certain areas (*e.g.*, children's media)?

2. Institutional Competence: Office of Technology?

Since creation of the FTC, the Bureau of Economics has guided the agency's understanding of economics. With technology issues increasingly dominating the FTC's agenda (measured in terms of priorities and impact, if not caseload), is it time for the FTC to institutionalize technological expertise in the same way it has institutionalized economic expertise – by creating a standing Office of Technology? It was not until late 2010 that the FTC appointed its first Chief Technologist, and the FTC remains without a full-fledged Office of Technology staffed with technologists, especially those from the business community who understand innovation tradeoffs. Indeed, its CTOs and senior advisors on technology have all been from academia, and the FTC might well benefit from an infusion of insight from those who have shaped technology in industry. It appears that the FTC draws on limited technical expertise scattered across multiple existing offices and bureaus, and on assistance from special contractors.

- What has been the track record of the FTC's first three Chief Technologists over the last three years?
- What does the institutional history of the Bureau of Economics suggest for how the FTC should approach building in-house technological expertise and using that expertise effectively in the various aspects of the FTC's enforcement, investigation and policymaking functions?
- What are the pitfalls of creating a larger permanent in-house technological capability? Might it cause the FTC to engage in more enforcement or use of the bully pulpit than is appropriate? How can such an office be integrated into all aspects of the FTC's work holistically as a resource to better weigh error costs? How can its expertise be married with an appropriate degree of humility about the ability of technical experts to predict an uncertain future?
- What kind of technical expertise would the FTC need to properly exercise the jurisdiction it has already asserted over broadband issues, such as Net Neutrality, speed claims and billing; over telecom services on all-IP networks; over privacy issues on telecom networks, if Congress transfers jurisdiction from the FCC; and over other telecom services?
- FTC computers do not have access to many new technologies, and some online services are actively blocked. Could such an office be used to better reform internal technology use at the FTC by, for example, improving its integration and use of new technologies?
- Could this office improve open data standards at the agency to allow researchers to engage in important consumer-welfare enhancing research (*e.g.*, non-sensitive Consumer Sentinel data)?

G. Codes of Conduct, Multistakeholder Processes & Advice Letters

Internet governance has, for decades, relied on multistakeholder processes, from ICANN's administration of the domain name system to the various standards-settings bodies that have shaped the technical framework that allows computers to connect over the Internet. Increasingly, policymakers have realized that such private, often highly informal bodies may be better source of law than traditional regulatory agencies when it comes to complex and fast-changing issues at the intersection of law and technology. Most notably, the White House's "Consumer Privacy Bill of Rights" declared that, "when appropriately structured … multistakeholder processes … can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges."[45] The Commerce Department has undertaken a series of government-sponsored processes, starting with mobile app transparency and continuing with facial recognition. But the private sector has increasingly been using such processes to generate codes of conduct, from the Digital Advertising Alliance's successful (if criticized) principles on behavioral advertising and multisite data to the W3C's still-unresolved Do Not Track Process. The FTC can enforce any promise to abide by such a code of conduct under its deception authority. Yet on many issues, it is widely presumed that substantive rules must come from the FTC, rather than being generated by such bodies and merely enforced by the FTC.

- What kinds of policy issues are better suited to resolution by multistakeholder bodies than by the FTC under unfairness or formal rulemaking, and under what circumstances?
- Why has no such code of conduct emerged regarding data security? Could the FTC's enforcement actions have displaced such bottom-up emergence of enforceable legal norms? Or are the data security requirements imposed by credit card networks upon vendors essentially the same thing?
- What systemic changes could the FTC make to encourage the emergence of codes of conduct from non-governmental sources? Has the agency's increasingly expansive conception of materiality in enforcing commitments to codes of conduct inadvertently discouraged the creation of such codes in the first place?
- Would the FTC need new statutory authority to recognize such codes of conduct (as proposed by the White House in draft privacy legislation) or could it recognize such codes informally by issuing advice letters, much as the Securities and Exchange Commission does?

IV. Substantive Issues

A. Competition

1. Antitrust law

At least since the Chicago revolution in antitrust, it has been generally acknowledged that antitrust is a blunt, powerful and thus potentially harmful instrument that requires significant analytical rigor to ensure it serves rather than undermines its consumer welfare objectives. In significant part because the antitrust laws are broad and vague they are easily misconstrued and misused. The Supreme Court's

[45] *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

recent antitrust jurisprudence has consistently recognized this and, almost without exception, operated to limit the scope of antitrust law and the discretion afforded to its enforcers.

In one sense antitrust is, in Herb Hovenkamp's description, a "residual" regulator, "promot[ing] competition to the extent that market choices have not been preempted by some alternative regulatory enterprise."[46] Implicit in this view of antitrust is a singular focus on private, as opposed to government, market restraints. Thus, unlike many other countries' competition laws and practices, U.S. antitrust law does not address public restraints as a matter of law enforcement, only as a matter of agency advocacy.

The FTC's enforcement of the antitrust laws has had mixed success, as is inevitable. Its existence is a function of early 20th Century Congressional expectations regarding the importance of specialized expertise in antitrust, but it isn't clear that the FTC has achieved particularly better results than, say, the Antitrust Division of the Department of Justice. Regardless, some have raised the question of the justification for the agency's existence (at least as an antitrust enforcer), particularly as its standards of enforcement (under the FTC Act) diverge from those of the DOJ (which does not enforce the FTC Act).

- There may be general agreement that antitrust merits some constraints, but the specific contours of those constraints are the subject of vigorous disagreement. With respect to the issues addressed in this report, are there particular judicial or legislative decisions that would optimize the constraints placed on the FTC's role in the antitrust enterprise?
- Former Chairman Leibowitz has argued (in advocating for expanded use of the FTC's UMC authority) that the limits imposed on antitrust by the Supreme Court are and should be aimed at private plaintiffs exclusively.[47] To the extent they constrain public enforcement these constraints are harmful and, thus, the appeal to Section 5 to sidestep the Court's jurisprudence is appropriate. Is this assessment appropriate? To what extent should government enforcers be subject to different judicial standards tan private plaintiffs?
    - In this regard, the FTC does enjoy a deferential standard of review for judicial review of the Commission's decisions on administrative adjudications. Is this deference appropriate? Does it help to ameliorate (or exacerbate) in any significant way the public/private enforcement question?
- Is the FTC's continued role in antitrust enforcement (alongside the DOJ) justified?
- Do the FTC's enforcement decisions reflect an appropriate role for economic analysis? Is the economics practiced at the FTC and embodied in its enforcement decisions and arguments the "right" economics?

[46] HERBERT HOVENKAMP, THE ANTITRUST ENTERPRISE (2005).

[47] *Interview: Federal Trade Commission's Jon Leibowitz*, Wall St. J. (Jan. 31, 2010) available at http://online.wsj.com/article/SB10001424052748704722304575037572444983454.html ("The courts have pared back plaintiffs' rights in antitrust cases. They're concerned about what they believe to be the toxic combination of class actions, treble damages and a very aggressive plaintiffs' bar. The problem for us as an agency is we come under those restrictions, [too]. So how do we do what we're supposed to do, which is stopping anticompetitive behavior? One tool in our arsenal is using what's known as our Section 5 authority to stop unfair methods of competition. When Congress created this agency, it wanted to give us broader jurisdiction to stop behavior that harms consumers than the antitrust laws. We haven't used it often recently but I think we're committed -- not necessarily often, but in appropriate circumstances -- to using this authority.").

- Of particular importance to antitrust's relationship with technology, do the FTC's enforcement decisions reflect an appropriate role for dynamic competition analysis, reflecting and rigorously applying an appreciation for difficult-to-observe and difficult-to-measure attenuated effects?
- Does the FTC make appropriate use of its administrative process in antitrust cases?

2. Unfair Methods of Competition

The FTC enforces the antitrust laws, the Sherman and Clayton Acts, only indirectly, by punishing violations of these acts – or more precisely, the complex web of judge-and-agency-made doctrines built upon these terse acts – as an "unfair method of competition." But what conduct, if any, does the FTC's UMC authority cover that the antitrust laws do not? Neither the courts nor Congress have ever resolved the question.

Increasingly the Commission has interpreted its UMC authority to extend the reach of the antitrust laws in novel fashion. These efforts have been met with considerable resistance. When, for instance, the majority in the Google SEP settlement asserted that conduct was unfair, but offered almost no explanation for why the conduct was unfair, it occasioned heated statements from Commissioners Ohlhausen and Rosch.[48] Two current Commissioners have proposed a Policy Statement on UMC analogous to those on DAP and UAP, and a third Commissioner has agreed, in principle, on the usefulness of such a statement. But the claimed need for UMC guidance is not without controversy.

It is an open question whether a UMC Policy Statement would, on net, reduce or increase the agency's competition enforcement power. While a Policy Statement would, as we have discussed generally, act as a constraint, Commissioner Wright and others have noted that self-restraint can actually *increase* the FTC's influence, even if it loses some degree of freedom.

- What should be the limiting principles of UMC? Should the same substantial injury requirement apply as in UAP cases?
- If Section 5 is in fact to prohibit conduct beyond the reach of the other antitrust laws, are guidelines necessary or advisable to delineate the scope of its jurisdiction as well as its economic basis?
- What kind of economic findings should be required to justify such guidelines? Specifically, what kind of empirical analysis would support finding that extending UMC beyond the antitrust laws would actually benefit consumers?
- If the FTC does not issue clear limiting UMC principles justified by adequate evidence, should Congress statutorily limit UMC to the Sherman Act?
- How should the Commission's definition of UMC inform its definition of UAP, and vice versa?
    - What are the conceptual parallels between UMC issues and, say, data security?
    - What role should economics, especially cost-benefit analysis have in both areas?

[48] In the Matter of Motorola Mobility LLC and Google Inc., FTC File No. 121-0120 (Ohlhausen, dissenting), *available at* http://www.ftc.gov/os/caselist/1210120/130103googlemotorolaohlhausenstmt.pdf (noting that "the majority says little about what 'appropriate circumstances' may trigger an FTC lawsuit); *id.* (Rosch, concurring), *available at* http://www.ftc.gov/os/caselist/1210120/130103googlemotorolaroschstmt.pdf ("[I]t is not clear what the 'limiting principles' of such a claim would be.").

3. Mergers

The FTC undertakes its merger enforcement activities largely in accordance with the familiar Horizontal Merger Guidelines. By almost all accounts, at least until the most recent, 2010 revisions, the Merger Guidelines have been successful. Since then-Assistant Attorney General Bill Baxter's 1982 Merger Guidelines,[49] the Merger Guidelines have largely embodied rigorous economic logic and operated to impose a degree of economic rigor on both the agencies and the courts. In fact, courts have looked to the Merger Guidelines in recent years as a source of law, thus reinforcing their internal constraining effect with a further external constraint. While the latest revisions to the HMGs are more controversial, there is little disagreement that the HMGs' influence on the FTC's merger enforcement practice (to say nothing of their usefulness for practitioners and the companies they advised) from 1984 until 2010 was salutary.

As noted, the 2010 revision to the Merger Guidelines introduced controversy in part – and in keeping with the theme of this report – because they also introduced more discretionary scope for the agency. Most notably, the new Guidelines contemplate an expanded scope for agency discretion in defining relevant markets and market power. Because courts have historically imbued the market definition/market power stage of merger analysis with near-dispositive significance, the new Guidelines' transformation of the traditional market definition analysis may, if broadly implemented by courts, undermine this constraint on agency merger enforcement discretion.

- To a significant extent, the 2010 Merger Guidelines do reflect recent agency practice, and in this sense fulfill an important function of guidelines. At the same time, by "codifying" the agency's more discretionary analytical framework they also have the potential to dramatically weaken the extent of the judicial constraint on agency discretion. Which of these two competing effects is more important to ensuring optimal merger outcomes? Are there specific changes to the 2010 Merger Guidelines that would rebalance that trade-off without undermining the Guidelines' descriptive accuracy?
- In terms of substance, do the Guidelines embody the appropriate economic framework for assessing the competitive effects of mergers? Could or should they do a better job continuing the legal retreat from the structure-conduct-performance model whose repudiation began with the 1982 Guidelines?
- The DOJ and FTC share authority for reviewing proposed mergers. Although there have been attempts to formalize the merger clearance process, none have had any staying power. Arguably, however, the informal process works. Should merger clearance be formalized to clarify for prospective merging parties which agency will review its merger?
- To some extent there are differences between the two agencies' merger processes and the process requirements imposed on the agencies in federal court. Do these different processes have significant practical effect on outcomes? Would harmonization be desirable – or possible?
- Merging parties bear monetary and disclosure obligations under the HSR Act, and merger reviews can be time intensive – creating substantial costs also borne by the parties. Are

[49] The 1982 Merger Guidelines were issued by the DOJ alone, but the *Statement of the Federal Trade Commission Concerning Horizontal Mergers* of the same year noted that "the DOJ 1982 revision to the 1968 Guidelines will be given considerable weight by the Commission and its staff." The FTC has joined the DOJ in issuing the HMGs since 1992.

premerger notification requirements appropriately calibrated to facilitate consummation of welfare-enhancing mergers while still enabling enforcement against anticompetitive mergers?

- How do we know? Does the FTC appropriately review and evaluate its merger practices?

B. Data Security

The FTC comes closest to being a "technology regulator" in data security cases. Through a string of four dozen UDAP enforcement actions over the last decade, the FTC has policed how American companies protect user data. Initially, the Commission used this standard only in deception cases, reading in an implied promise of reasonableness into data security promises and holding companies responsible if actual practice was found to be unreasonable. Since 2005, however, the FTC has expanded the reasonableness approach to cases in which the company made no security promise, essentially collapsing UAP's substantial injury/countervailing benefit/reasonably avoidable elements into "reasonableness," which in turn has largely, if not explicitly, been defined by the data security standards (the "Safeguards Rule") promulgated through APA rulemaking for financial institutions under Gramm-Leach-Bliley.

In principle, it makes sense treat some forms of inadequate data security as an unfair trade practice, regardless of whether the company made any promise about security. But recent experience suggests the FTC is moving toward *ex post* strict liability and away from judging the reasonableness of security precautions *ex ante*, and making that assessment without first developing or explaining the elements of unfairness in a rigorous way. While companies, such as Wyndham, and many commentators have argued for the need for greater guidance, it is not clear what shape that guidance should take.

Although some have argued that the agency's data security complaints, consent orders, speeches and Congressional testimony collectively provide sufficient guidance, the lack of more formal guidelines is notable.[50] Moreover, this set of guiding materials is notably lacking any direct discussion of the reasons data security investigations are *closed* (and none are likely to appear in the near future given a relatively new informal policy strongly disfavoring such explanations).

- Is the FTC's approach becoming a strict liability rule, presuming that any loss of data is *per se* proof that a company's data security practices were unreasonable? If so, on what legal basis?
- In practice, the FTC brings data security cases (under both Deception and Unfairness) based on the alleged unreasonableness of a respondent's security practices without addressing the actual Section 5 elements (materiality, substantial injury, *etc.*) and without connecting them to reasonableness. Would making such connections explicit satisfy the need for flexibility as well as certainty? Put differently, is the need for "standards" more a need for doctrinal guidance (about how the FTC measures reasonableness) than for specific technical measures or requirements?
    - Would a policy statement or other doctrinal guidelines on data security help to provide clearer notice about what constitutes reasonable data security, taking account of the need for experimentation, self-correction, consumer self-help and the costs and

[50] Some have further argued, in fact, that that the threat of action through speeches, reports and the like is preferable to more concrete statements or guidelines because they are even more flexible. *See, e.g.*, Tim Wu, *Agency Threats*, 60 DUKE L.J. 1841 (2011), http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1506&context=dlj.

benefits of data security practices with reference to other characteristics (like company size, industry, threat, *etc.*)?
    - Or does the Commission need to provide greater guidance on UAP more beyond just data security cases, to further explain how the Commission will implement the principles of the Unfairness Policy Statement? How would such guidelines compare with antitrust guidelines?
    - If consent decrees are to be the primary form of guidance the FTC offers to companies, can the FTC better explain how it weighs the required elements of unfairness in each complaint or other materials explaining the settlement?
- Would greater *ex ante* certainty (in whatever form) sacrifice too much flexibility, perhaps imposing far greater costs on businesses and consumers than the current regime? How should the Commission evaluate the trade-off between certainty and flexibility?
- What are the appropriate boundaries of substantial injury? If the FTC's cases rely on losses borne by companies (fraudulent charges reimbursed to consumers), is the FTC really protecting consumers or large businesses? Consumers can, and do, suffer out of pocket losses, particularly with new account fraud. How great must they be to constitute substantial injury?
- What about the time and effort required to mitigate harm, such as monitoring account charges or replacing credit cards? How should this be measured as a form of injury or as part of the inquiry into whether consumers can "reasonably avoid" injury?
- Is the guidance provided in the Safeguards Rule – which, while offering some details, nonetheless ultimately rests on operative rules like "Reasonable" and "effective" – the appropriate amount of specificity and guidance necessary in data security and other fast-paced issues?
- Regardless, is it appropriate for the FTC to boot-strap a rule enacted under one statute to direct FTC enforcement action under Section 5?
- In particular, if reasonableness depends, under the Safeguards rule, on the specific characteristics of the company, has the FTC provided enough guidance as to those characteristics?
- How should the Commission apply its standards to ensure that the duty of care imposed on businesses is appropriate to their size and degree of sophistication, as well as to the security threats at issue?

C. Patents

Perhaps nothing the FTC does more directly implicates technology and innovation than its treatment of intellectual property. Writing about "Antitrust in the New Economy," Judge Posner noted that the "principal output of these industries... is intellectual property."[51] But as far as antitrust economics has progressed generally, it still lacks a solid understanding of the relationship among investment in R&D, market structure, price, quality, speed of innovation and welfare effects. The risk of Type 1 error thus is particularly high, and its potential cost higher still.[52] Nonetheless, basic economics suggests that, in unknown degrees, the production, distribution and enforcement of intellectual property will lead to

[51] Richard A. Posner, *Antitrust in the New Economy*, 68 ANTITRUST L.J. 925, 927 (2001).

[52] Manne & Wright, *Innovation*, *supra* note **Error! Bookmark not defined.**, at 170.

standardization (coordination among competitors), the need for interoperability (and thus a greater opportunity for anticompetitive foreclosure), economies of scale (high levels of concentration), and the presence of network effects, all of which may contribute to an increased likelihood of monopolization.[53] On the other hand, many question the validity of many patents and the reliability of the patent approval process, and note the potential for "greenmail." These critics have encouraged the FTC to use its UMC authority against companies asserting legally questionable or standard-essential patents (SEPs) in certain contexts.

Against this backdrop, the FTC has in recent years stepped up its enforcement around patents. Recent (and controversial) Section 5 cases against Intel, Rambus, Google and Bosch, for example, have turned on issues surrounding those firms' enforcement of SEPs. The Commission is currently conducting a 6(b) investigation into patent assertion entities, and the FTC has pursued a vigorous and lengthy war on pharmaceutical industry reverse payment settlements.

The question of the appropriate application of UMC to patent issues, particularly to police the enforcement of SEPs through the threat of injunctions and the breach of FRAND requirements by certain patent holders, is a controversial one. But here as elsewhere the core of the controversy may rest in the appropriate exercise of discretion generally rather than as applied to patents in particular. As Commissioner Ohlhausen wrote in dissenting from the Commission's action in *Bosch*:

> I simply do not see any meaningful limiting principles in the enforcement policy laid out in these cases. The Commission statement emphasizes the context here (*i.e.* standard setting); however, it is not clear why the type of conduct that is targeted here (*i.e.* a breach of an allegedly implied contract term with no allegation of deception) would not be targeted by the Commission in any other context where the Commission believes consumer harm may result.[54]

Whatever the propriety of the application of Section 5 to these issues, there remains important questions regarding the appropriate *scope* of that authority.

- The upshot of the FTC's range of actions against patents is, in varying degrees, to move the property rule of patents (enforceable by injunction) more towards a liability rule (enforceable by royalty payments). Is such a shift justified? Is it beneficial or harmful?
- To the extent that the FTC's SEP actions are motivated by concerns about "hold-up" problems arising from refusals to license essential IP, is the FTC sufficiently sensitive to the analogous "hold-out" problem of potential licensees taking advantage of lax enforcement in order to infringe?
- Is the FTC applying its approach to patents consistently? Or has it unfairly singled out a class of patents or patent-holders?
- Is the FTC's overall patent-related activity essentially a form of competition advocacy directed at the USPTO, Congress and the courts? What would more direct competition advocacy in this area look like and would it be preferable?

[53] *Id.*

[54] In the Matter of Robert Bosch GmbH, FTC File No. 121-0081 (Nov. 26, 2012) (Maureen Ohlhausen, dissenting), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-ohlhausen/121126boschohlhausenstatement.pdf.

- Related, many (including many in Congress) see significant problems in the patent system. To the extent that patent system problems rather than competition problems underlie the FTC's patent-related actions, does this represent an appropriate exercise of the agency's power? Is the agency sufficiently sensitive to the scope of its authority vis-à-vis other agencies and branches of government?

- Should the FTC be responsible for regulating the demand letter process under its UMC authority, as some have proposed? What are the advantages and pitfalls of such an approach?

D. Advertising & Pure Deception

The core of the FTC's consumer protection work lies in policing deception in marketing and advertising claims, where it enjoys broad support as ensuring that consumers get the benefit of the deal they were promised. The Commission thus protects consumers from a clear injury, yet it need not prove any actual or even likely injury in any enforcement action because, so long as a statement to the consumer was material to their decision, the Commission may validly presume that *not* getting what the statement promised constitutes harm.[55] Yet the FTC's recent enforcement actions have raised two concerns regarding its application of deception: (1) the degree of substantiation required, particularly for health claims, and (2) the FTC is pushing the boundaries of its deception authority by attempting to enforce statements that are not clearly material to consumers, and thus where harm cannot be presumed.

1. Advertising Labeling

The FTC has a long history of both advocacy about and enforcement against what it has deemed insufficient labeling of messages as advertising. This effort has intensified as technology has disrupted traditional means of communicating to consumers: from its Endorsement Guidelines to its Search Labeling Letters to its recent Native Advertising Workshop. Some failures to label a message as an advertisement are clearly misleading to consumers. However, many have criticized some of the Commission's recent guidelines as stifling free speech, failing to adequately assess whether consumers are injured, and advocating conduct that is not clearly required by the law.

- Is the FTC seeking disclaimers about speech that are moored in journalistic ethics rather than in Section 5?
- Is the FTC guidance here appropriately allowing for innovative labeling techniques? Or is the FTC creating inflexible guidelines that push for certain formats and unneeded consistency?
- Is the FTC properly assessing costs to free speech, innovation, and burden on content providers in its advocacy? Again, what has BE's role been in assessing the FTC's approach in this area?
- Is the FTC properly considering the context of the speech when determining what constitutes proper labeling?

Is the FTC focusing its resources on activity and actors that are most clearly deceptive and likely to cause consumer harm?

[55] Deception Statement, *supra* note 15.

2. Claim Substantiation Standards

The FTC recently reversed a decision of its Administrative Law Judge holding that POM Wonderful had adequately substantiated the health claims it made in marketing its signature pomegranate juice by spending more than $30 million on scientific research. Instead, the FTC held, for the first time in the agency's history, that such claims must be backed by randomized clinical trials of the sort required of drug makers, who spend an average of $600 million on RCTs. There is little change such massive costs could be recouped in a competitive market, especially because companies like POM cannot patent their food products the way drug makers can. So the FTC's RCT requirement amounts to a ban on an entire category of speech.[56] The FTC decision also seems to contravene the D.C. Circuit's 1999 decision in *Pearson v. Shalala*, where the court struck down a similar FDA requirement and required the FDA to allow health benefit claims if made with appropriate qualifications alerting the public to the lack of conclusiveness in the science.[57]

- In reaching this decision, how did the FTC weigh the costs and benefits of effectively banning health claims like those made by POM Wonderful?
- In general, how well substantiated must a claim be to avoid being subject to a deception action? What burden does the FTC bear in substantiating its own deception claims with economic evidence?
- Does an adjudicatory process allow for proper weighing of such evidence, or should the Commission use its rulemaking process to ensure a proper weighing of the record?

3. The Presumption of Materiality

In traditional advertising, the FTC applies a second presumption: that all advertising claims were material. But increasingly, the Commission is extending that presumption of materiality to claims made outside advertising, in forms ranging from privacy policies to online help file to FAQs. For example, FTC alleges that the "unreasonable" data security of Wyndham's hotels was both itself an unfair trade practice and also deceptive, insofar as it violated the company's promise to "safeguard [its] Customers' personally identifiable information by using industry standard practices." The FTC is thus trying to hold Wyndham responsible for deception despite an explicit disclaimer in the same privacy policy that the parent company was not responsible for the data security practices of its franchisees. At oral argument, FTC Counsel asserted, flatly, that "expressed statements are presumed material under FTC law."[58] In another case, the FTC charged Google with having violated a consent decree by deceiving customers

[56] Members of the Working Group filed two amicus briefs in this matter. *See* Brief of Amici Curiae Consumer Healthcare Products Association & Council for Responsible Nutrition in Support of Petitioners' Request for Reversal, No. 13-1060 (Aug. 21, 2013), *available at* http://www.crnusa.org/pdfs/r_8475.pdf; Brief of Amici Curiae Alliance for Natural Health-USA & TechFreedom Supporting Petitioners' Opening Brief, no. 13-1060 (Aug. 20, 2012), *available at* http://techfreedom.org/post/58924602984/pom-wonderful-ftc-ban-on-food-health-claims-violates.

[57] Pearson v. Shalala, 164 F.3d 650 (D.C. Cir. 1999).

[58] Oral argument transcript in FTC v. Wyndham, at 132, *available at* http://www.pogowasright.org/wp-content/uploads/FTC_V._WYNDHAM_OralArgument-.pdf.

after an online help page explaining how Apple users could configure their browser to block Google cookies became inaccurate due to technical changes made by Apple.[59]

- The 1983 Deception Policy Statement says that "In many instances, materiality, and hence injury, can be presumed from the nature of the practice" but adds that, "In other instances, evidence of materiality may be necessary."[60] When does it make sense for the FTC to presume all express statements are material? If it cannot make such a presumption, how should it determine whether a statement is actually material? What role should economics play in such determinations?
- How does the FTC weigh the potential for over-enforcement of deception to discourage companies from making statements in the first place?

E. Privacy

The Commission's approach to privacy issues beyond data security has been more amorphous. While the Commission has brought a number of privacy-related enforcement actions, they are not as uniform in their concerns, approach or remedies as the Commission's data security cases. The Commission's approach to privacy has been dominated by its 2010 Privacy Report,[61] as well as the various workshops that led to that report and that have followed, building on the report in other areas, such as the Internet of Things. Certain Commissioners have continued to call for "baseline comprehensive privacy legislation," and the Obama Administration appears ready to introduce their own draft legislation imminently. Meanwhile, a bipartisan House task force is examining the question of privacy.

The FTC has also played a significant role in ongoing private sector efforts to produce privacy codes of conduct. Most notably, the World Wide Web Consortium's Tracking Protection (Do Not Track) Working Group was driven to a large degree by pressure from the FTC and some participants have suggested that FTC pressure for the chairs to produce particular outcomes may have made a negotiated outcome with industry impossible.

- What economic analysis of trade-offs, and what legal analysis of underlying doctrines, did the FTC engage in its 2012 Privacy Report?
- Do such reports help guide industry in complying with their legal obligations under Section 5? Or, given their lack of discussion of legal basis, are they primarily hortatory, recommending best practices that the FTC cannot actually require? Is the FTC sufficiently clear when its guidelines are merely "best practices" rather than required by law?
- When holding workshops and creating guidelines, is the FTC openly assessing all views? Or is it steering the record toward a pre-determined result?

---

[59] Federal Trade Commission, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Apple's Safari Internet Browser*, Press Release (Aug. 9, 2012), http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[60] Deception Statement, *supra* note 15.

[61] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 2010), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

- Is it, in fact, necessary for the FTC to steer clear of any consideration of how access by law enforcement or national security affect privacy, as it has routinely insisted it must? Or, since the FTC has general authority to collect information and advocate for policies that remove barriers to competition and enhance consumer welfare, should the FTC take a more holistic view of privacy in its reporting, analysis and recommendation functions?
- What does the FTC's experience with privacy regulation thus far and with other grants of statutory authority, especially COPPA, tell us about the advantages and disadvantages of "comprehensive" privacy legislation? How should economic analysis and an understanding of error costs guide the FTC's discretion in fleshing out a statutory framework through regulation and enforcement?
    - How well did the FTC justify its expansion of the COPPA rule? What role did economics, and the Bureau of Economics, play in this process?
- What does the history tell us about the advantages and pitfalls of giving the FTC statutory authority to certify safe harbors from enforcement of comprehensive baseline privacy legislation, as apparently proposed by the White House bill? In particular, given that merger reviews at the FCC and, increasingly, antitrust reviews generally at the FTC and DOJ, frequently result in companies "voluntarily" agreeing to settlements that involve major concessions that the agencies could not legally (or in some cases, even constitutionally) have required, might such a process give the FTC too much discretion in defining the terms of codes of conduct? Where is the line between "self-regulation" or truly bottom-up multistakeholder processes and "co-regulation?"
- Is the FTC focusing its resources on consumer protection issues that result in concrete consumer harm, or engaging more broadly in privacy policy development that is not based on whether the practices in question create specific harms to consumers?

V. Conclusion

The FTC enjoys uniquely broad support across political and ideological lines for its mission: maximizing consumer welfare through its consumer protection and competition powers. The issues presented in this report are just some of the many questions that must be considered by the FTC and Congress as the Commission approaches its 100th anniversary in September 2014. Without serious consideration of these questions, and without whatever reforms are implied by their answers, the agency risks failing to reach its otherwise positive potential.

Above all, achieving that potential depends on understanding that too much discretion can actually weaken the agency's ability to execute its mission – and that limits, imposed internally or externally, can significantly strengthen the agency's ability to succeed. Greater analytical discipline and legal rigor will help the agency provide clearer guidance, thus promoting compliance while minimizing the burden of regulation; it will also help the agency prioritize its limited resources and ensure that it can enforce the law vigorously within the scope of its legal authority and general principles of the rule of law.

The **FTC: Technology & Reform Project** brings together a unique collection of experts on the law, economics, and technology of competition and consumer protection to consider challenges facing the FTC in general, and especially regarding its regulation of technology.

This document represents the combined input of several authors and commentators, and has been complied to ask questions and prompt discussion about the Federal Trade Commission. It is, by design, over-inclusive, so that it may foster broad discussion. At the same time, it is also certainly not complete. This document does not necessarily represent the views of its principal authors or other contributors to the drafting process, nor the members of the FTC: Technology & Reform Project.

Project Members:

- **Howard Beales**, Professor, George Washington University; Former Director, Bureau of Consumer Protection
- **Terry Calvani**, Of Counsel, Freshfields Bruckhaus Deringer LLP; Former Commissioner, Federal Trade Commission
- **James Cooper**, Director of Research and Policy, Law and Economics Center at George Mason University School of Law; Former Acting Director, Office of Policy Planning
- **Jeffrey Eisenach**, Visiting Scholar, Center for Internet, Communications and Technology Policy at the American Enterprise Institute; Former Economist, Bureau of Economics
- **Gus Hurwitz**, Assistant Professor of Law at University of Nebraska College of Law
- **Tad Lipsky**, Partner, Latham & Watkins; Former Deputy Assistant Attorney General, Department of Justice
- **Geoffrey Manne**, Executive Director, International Center for Law & Economics
- **Timothy Muris**, GMU Foundation Professor of Law, George Mason University School of Law; Former Chairman, Federal Trade Commission
- **Paul Rubin**, Samuel Candler Dobbs Professor of Economics, Emory University; Former Director of Advertising Economics, Federal Trade Commission
- **Joanna Shepherd-Bailey**, Associate Professor of Law, Emory University School of Law
- **Joe Sims**, Partner, Jones Day; Former Deputy Assistant Attorney General, Department of Justice
- **Gerry Stegmaier**, Of Counsel, Wilson Sonsini Goodrich & Rosati
- **Berin Szoka**, President, TechFreedom
- **Sasha Volokh**, Assistant Professor of Law, Emory University School of Law
- **Todd Zywicki**, GMU Foundation Professor of Law, George Mason University School of Law; Former Director, Office of Policy Planning

Testimony of
Berin Szoka, President
TechFreedom[1]

on

Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?

Before the House Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade[2]
March 29, 2012

I. Introduction

The central challenge facing policymakers is three-fold:

- Defining what principles should govern privacy policy;
- Transposing those principles into concrete rules, whether through self-regulation or legislation, and updating them as technology changes; and
- Determining how to effectively enforce compliance.

Unfortunately, the privacy debate has until now focused mostly on the first part, crafting the right principles. Both President Obama's proposed "Consumer Data Privacy Framework"[3] and the FTC's Report[4] do wisely recognize not only the central importance of the second part (transposition from the abstract to the concrete), but also that the "flexibility, speed, and decentralization necessary to address Internet policy challenges"[5]—like balancing the dangers of data with its benefits—can come only from a self-regulatory process such as the Commerce Department has proposed to facilitate.[6]

---

1 Berin Szoka (@BerinSzoka) is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on consumer privacy. In particular, he testified on COPPA before the Senate Commerce Committee on April 29, 2010, available at http://tch.fm/syexUo, ("Szoka Testimony").

2 http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=9404

3 The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy ("White House Report"), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

4 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("FTC Report"), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

5 White House Report at 23.

6 National Telecommunications and Information Administration, Request for Comments, *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct* ("NTIA RFC"),

But both the White House and FTC propose principles that, while noble in their aspirations, may prove counter-productive for consumers if transposed without a careful consideration of the real world trade-offs inherent in regulating consumer data practices. Both documents present reformulations of the Fair Information Practice Principles. While the White House framework is perhaps the best articulation of the FIPPs thus far, the FIPPs alone cannot protect consumers effectively—at least not without imposing significant costs and burdens on consumers. The devil lies in effective transposition. As the Cato Institute's Jim Harper puts it so eloquently puts it:

> Appeals to the [FIPPs] are a ceremonial deism of sorts, boilerplate that advocates use when they don't know how to give consumers meaningful notice of information policies, when they don't know when or how consumers should exercise choice about information sharing and use, when they don't know what circumstances justify giving consumers access to data about them, and when they don't know how to describe which circumstances—much less which systems or what levels of spending—make personal data sufficiently "secure."[7]

Moreover, neither the White House nor the FTC adequately explores the legal authority and institutional capacity necessary to achieve effective enforcement, the real heat of the privacy problem. On capacity, Congress has a vital role to play in ensuring that the FTC has a clear plan to develop the in-house technical capacity it needs to keep pace with technological change and the resources needed to implement that plan.

Importantly in this regard, developing the capacity to understand and effectively regulate technology is as much about ensuring that regulators understand how innovative technology confers benefits on consumers as it is about ensuring that regulators understand how new technology *doesn't* impose imaginary costs. As technological advance brings about ever more effective means of collecting and analyzing information, there is a tendency to view this through the lense of harm—to see such advances as ever more intrusive and potentially harmful. Forty years ago, the great economist Ronald Coase warned us: "If an economist finds something—a business practice of one sort or another—that he does not understand, he looks for a monopoly explanation. And as in this field we are very ignorant, the number of understandable practices tends to be very large, and the reliance on a monopoly explanation, frequent."[8] The same risk arises here—that, finding a technology that they don't understand, regulators will look for a nefarious (or "unfair") explanation, overestimating harms to users (the more easily seen) and understating benefits (the more likely unseen).[9] Ensuring that regulators

---

https://www.federalregister.gov/articles/2012/03/05/2012-5220/multistakeholder-process-to-develop-consumer-data-privacy-codes-of-conduct.

[7] Jim Harper, *Reputation Under Regulation: The Fair Credit Reporting Act at 40 and Lessons for the Internet Privacy Debate*, Cato Policy Analysis No. 690 (Dec. 8, 2011), http://www.cato.org/pubs/pas/PA690.pdf.

[8] Ronald Coase, *Industrial Organization: A Proposal for Research*, in 3 Policy Issues and Research Opportunities in Industrial Organization, 59, 67 (Victor Fuchs ed. 1972).

[9] See Frederic Bastiat, *What Is Seen and What Is Not Seen*, http://www.econlib.org/library/Bastiat/basEss1.html

have the capacity to keep up with technological change is thus essential to facilitating both effective and appropriately restrained enforcement.

On authority, the FTC could do more with its existing unfairness authority to build a quasi-common law through enforcement actions and written guidelines on consumer data practices that cause greater consumer injury than benefit and which consumers themselves cannot reasonably avoid. The Unfairness Doctrine is a powerful tool by which the FTC can punish either practices not addressed by self-regulation or companies that simply choose not to abide by self-regulation. But it is precisely because this tool is so powerful that its use was carefully limited by the FTC in 1980—and should remain so.[10] If the Unfairness Doctrine proves too limited in the non-economic harms it recognizes, Congress should craft legislation narrowly tailored to those harms, rather than allowing the FTC to expand the scope of the Unfairness Doctrine in general. But even in legislating based on a somewhat broader conception of harm, Congress should heed the basic approach of the Unfairness Doctrine, which remains a sound basis for effective consumer protection: weigh consumer harm against consumer benefit and intervene only where consumers themselves cannot reasonably avoid the harm, such as through their own use of more effective privacy controls.

If Congress is ever to grant the FTC new authority in this area, it should at least wait to learn from the self-regulatory process. Congress should assess the failure or success of the overall self-regulatory system in three ways:

1. **Enforcement**: Can compliance with self-regulatory codes of conduct be policed effectively? If not, how can industry self-enforcement of self-regulation be strengthened? And how can FTC enforcement based on deception be enhanced?
2. **Outside Self-Regulation**: Can companies that remain outside self-regulation be policed effectively? If not, to what extent is the problem that the FTC lacks institutional capacity to use its unfairness authority effectively or that its legal authority is too limited because the limits on the Unfairness Doctrine make successful litigation too difficult?
3. **Scope & Evolution**: Does self-regulation adequately address privacy practices that, on net, harm consumers and cannot be reasonably avoided by consumers themselves?

In the first two cases, policymakers would do well to heed the paraphrase of an old adage about malice:[11] never attribute to a lack of legal authority that which can be adequately explained by a lack of institutional capacity. Of course, institutional capacity only goes as far as the FTC's legal authority, but where capacity is lacking, how can we know whether authority is really inadequate?

---

[10] FTC Policy Statement on Unfairness ("Unfairness Policy Statement"), appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). See 15 U.S.C. § 45(n).

[11] Hanlon's Razor is an eponymous adage that reads: "Never attribute to malice that which is adequately explained by stupidity." See, e.g., http://en.wikipedia.org/wiki/Hanlon's_razor.

II. A "Bill of Rights" for Consumer Privacy?

It was President Kennedy who first introduced a Consumer Bill of Rights in a speech to Congress in 1962.[12] So it is hardly unprecedented that President Obama should choose a similar label for his consumer privacy framework. No doubt this is a highly effective rhetorical framing that will drive action—whether by industry or Congress—on this complicated and often arcane topic. But the "Bill of Rights" term is problematic in two senses.

First, the Report begins and ends as constitutional sleight-of-hand. President Obama starts by reminding us of the Fourth Amendment's essential protection against "unlawful intrusion into our homes and our personal papers"—by government. But the Report recommends no reform whatsoever for outdated laws that have facilitated a dangerous expansion of electronic surveillance. In other words, while the White House embraces the "Consumer Bill of Rights" rhetoric, the *real* Bill of Rights is in peril. This was precisely the message sent by a unanimous Supreme Court two months ago in its *Jones* decision.[13] Indeed, five Justices called on Congress to remedy this situation by updating outdated laws intended to implement the Fourth Amendment's protections in digital technologies.[14] The gravest threat to our privacy comes from Congress's failure to enact such reforms—while instead focusing its limited attention on legislation mandating that private companies retain *more* information about how we use the Internet, which law enforcement could access without judicial scrutiny,[15] and cybersecurity legislation designed to facilitate the monitoring of user communications.[16] Unfortunately, the White House Report dismisses such concerns in the first footnote.[17]

Second, conceptualizing privacy in "rights" terms, while emotionally appealing, is deeply problematic. The rights contained in the *real* Bill of Rights stand between us and our government, whose proper purpose is to protect our negative rights to life, liberty and the pursuit of happiness. "Rights" are, in philosophical parlance, often conceived as "trumps" over mere "interests"—in other words, not subject to trade-offs or balancing, except perhaps with

---

[12] John F. Kennedy, 93 - Special Message to the Congress on Protecting the Consumer Interest, Mar. 15, 1962, *available at* http://www.presidency.ucsb.edu/ws/?pid=9108.

[13] U.S. v. Jones, 565 US __ (2012), http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

[14] Id.; Berin Szoka & Charlie Kennedy, *Supremes to Congress: Bring Privacy Law Into 21st Century*, CNET, Jan. 29, 2012, http://news.cnet.com/8301-13578_3-57368025-38/supremes-to-congress-bring-privacy-law-into-21st-centur/.

[15] Berin Szoka, *Leading Free Market Groups Urge Congress to Update Key U.S. Privacy Law*, TechFreedom, April 6, 2011, http://techfreedom.org/blog/2011/04/06/leading-free-market-groups-urge-congress-update-key-us-privacy-law.

[16] Cybersecurity Act of 2012, 112th Congress (2012), http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105; Jim Harper, *The Senate's SOPA Counterattack?: Cybersecurity the Undoing of Privacy*, Cato@Liberty, Feb. 9, 2012, http://www.cato-at-liberty.org/the-senates-sopa-counterattack-cybersecurity-the-undoing-of-privacy/.

[17] "This framework is concerned solely with how private-sector entities handle personal data in commercial

se ttings. A separate set of constitutional and statutory protections apply to the government's access to data that is in the possession of private parties." White House Report at 5 n. 1.

other rights.[18] This is essentially the European conception of privacy as a "fundamental human right." It conceives of privacy as a positive right, rather than the sort of negative right recognized under U.S. law. It is also essentially a property right in personal information, a problematic concept when applied to personal information.[19]

III. The Power, Risks and Benefits of Data

The privacy debate rests on a recognition of the growing power of data to shape our lives. But largely because of the conceptualization of privacy as a positive (fundamental) right, or a strict property right in personal information, the privacy debate has been systematically biased by an over-statement of the risks and an under-statement of the benefits of data. A more realistic debate would begin by weighing real privacy harms (a subject discussed below in the context of the FTC's Unfairness Doctrine) with information benefits such as:

- Enhanced advertising revenues for publishers of content and services that might otherwise have difficulty funding their offerings by charging for data, especially in markets where marginal costs are lower or zero (and basic economic theory would suggest that competition will inevitably drive prices towards zero).
- More effective advertising, which in turn means
    - More relevant, and potentially less annoying/interruptive advertising for consumers;
    - Better correlation between the production of content and services, and consumer
    - preferences;
    - Lower prices for consumers and greater innovation throughout the economy;
    - Better non-commercial messaging, too; and
    - More vibrant media and improved political discourse and communities[20]
- Serendipitous innovation based on the discovery of unexpected uses of data.

As discussed below, the FTC's existing Unfairness Doctrine provides a sound vehicle for weighing harms with benefits, and regulating only where users cannot reasonably avoid a harmful practice. But more generally, balancing risks realistic assessment of the degree to which a particular data set is likely to be tied back to a particular user at all.

---

[18] Leif Wenar, "Rights", The Stanford Encyclopedia of Philosophy (Fall 2011 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/fall2011/entries/rights/#5.1.

[19] *See generally* Larry Downes, *The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age* 70-71 (2009).

[20] *See generally* Berin Szoka, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech,* Comments the FTC Privacy Roundtables (Dec. 7, 2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00035.pdf

IV. PII, Anonymization & Re-Identification

The FTC's 2010 Preliminary Staff Report hinted that the agency might abandon the traditional distinction between PII and non-PII on the grounds that relevance of this distinction is decreasing as it becomes possible to identify anonymous datasets, or to re-identify de-identified data.[21] But in the face of criticism, the final FTC Report changed course and clarified that "data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." This is an eminently sensible compromise.

While the White House Report does not explicitly address the debate that has raged behind this reversal of positions, nor does it emphasize the importance of de-identification in general, it does specifically call for de-identification as a core element of its "Transparency"[22] and "Focused Collection"[23] principles.[24]

Ensuring proper de-identification should be a core goal of self-regulation—and legislation, if that proves necessary. Balancing realistic risks of re-identification with a realistic assessment of harms likely to flow from re-identification is essential to ensuring that privacy regulation (and self-regulation) benefits consumers. As Brooklyn Law School professor Jane Yakowitz explains in her seminal 2011 law review article, Tragedy of the Data Commons:

> Accurate data is vital to enlightened research and policymaking, particularly publicly available data that are redacted to protect the identity of individuals. Legal academics, however, are campaigning against data anonymization as a means to protect privacy, contending that wealth of information available on the Internet enables malfeasors to reverse-engineer the data and identify individuals within them. Privacy scholars advocate for new legal restrictions on the collection and dissemination of research data. This Article challenges the dominant wisdom, arguing that properly de-identified data is not only safe, but of extraordinary social utility. It makes three core claims. First, legal scholars have misinterpreted the relevant literature from computer science and statistics, and thus have significantly overstated the futility of anonymizing data. Second, the available evidence demonstrates that the risks from anonymized data are theoretical - they rarely, if ever, materialize. Finally, anonymized data is crucial to

---

[21] FTC 2010 Report at 39.

[22] "[C]ompanies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or *de-identify it from consumers*, and whether and for what purposes they may share personal data with third parties." White House Report at 14 (emphasis added).

[23] "Companies should securely dispose of or *de-identify personal data once they no longer need it*, unless they are under a legal obligation to do otherwise." White House Report at 21 (emphasis added).

[24] The Report also notes that the Department of Health and Human Services "plans to issue additional guidance on the HIPAA Privacy Rule's "minimum necessary" standard and on de-identification of health information under the HIPAA Privacy Rule. White House Report at 43.

> beneficial social research, and constitutes a public resource - a commons - under threat of depletion. The Article concludes with a radical proposal: since current privacy policies overtax valuable research without reducing any realistic risks, law should provide a safe harbor for the dissemination of research data.[25]

V. Individual Control

The White House's first principle is that "Consumers have a right to exercise control over what personal data companies collect from them and how they use it." This is probably the most viscerally compelling principle[26] but is deeply problematic if understood as a "right" to be strictly enforced rather than an aspirational principle to be transposed pragmatically, depending on the trade-offs inherent in the real world. Hence, the vital importance of the word "appropriate."

The concept has its roots in the original 1890 law review article by Warren and Brandeis that gave birth to modern privacy law, where they declared that:

> Recent inventions & business methods call attention to... the right "to be let alone." Instantaneous photographs & newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops.'"[27]

By contrast, the Supreme Court ruled in 1967 that:

> Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press.[28]

In other words, much as we might want a right to keep people from speaking about us, we do not have, as the White House Report suggests if read literally, "a right to exercise [*absolute*] control over what personal data companies collect from [us] and how they use it."[29] UCLA Law professor Eugene Volokh explained this best in his seminal 2000 law review article, "Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You.":

---

[25] Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. J. of Law & Tech 1 (Fall 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749.

[26] "Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves." Jim Harper, Cato Institute, Understanding Privacy – and the Real Threats to It, Cato Institute Policy Analysis No. 520, Aug. 4, 2004, http://www.cato.org/pub_display.php?pub_id=1652.

[27] Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (Dec. 15, 1890), *available at* http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[28] Time, Inc. v. Hill, 385 U.S. 374, 388 (1967).

[29] White House Report at 1.

> Government attempts to let us "control … information about ourselves" sound equally good: Who wouldn't want extra control, especially of things that are by hypothesis personal? And what fair-minded person could oppose requirements of "fair information practices"?
>
> The difficulty is that the right to information privacy—the right to control other people's communication of personally identifiable information about you—is a right to have the government stop people from speaking about you. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from "control[ling the communication] of information" (either by direct regulation or through the authorization of private lawsuits, whether the communication is "fair" or not. While privacy protection secured by contract turns out to be constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.[30]

There are also real costs to choice, and benefits of having no choice, as Indiana University Law professor Fred Cate argues in his essay, "The Failure of Fair Information Practice Principles":

> In some cases, consent may be undesirable, as well as impractical. This is true of press coverage of public figures and events, medical research, and of the many valuable uses of personal information where the benefit is derived from the fact that the consumer has not had control over the information. This is certainly true of credit information: its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make the credit report useless.[31]

These practical and constitutional realities are already recognized by U.S. privacy law. The Fair Credit Reporting Act, for example, does not allow us to control what others say about our credit history, but instead gives us access and correction rights to make sure the information on which they base what they say about us is accurate.[32] This is premised not on our ownership of "our" information, but on the clear harms that can follow from inaccurate speech about us. While the FCRA is far from perfect,[33] it is at least an example of how a harms-based approach can serve as the basis for preventing harmful uses of information about us. And this example illustrates that even a principle as appealing as individual control cannot be treated as a "right" but must be transposed carefully to apply to a particular privacy problem.

---

[30] Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 1999, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200469.

[31] Fred H. Cate, *The Failure of Fair Information Practice Principles*, 2006, *available at* http://ssrn.com/abstract=1156972.

[32] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., *available at* http://www.ftc.gov/os/statutes/031224fcra.pdf.

[33] Harper, *Reputation Under Regulation, supra* note 7.

VI. Transparency

In some ways, the transparency principle is perhaps universally embraced in the White House Report. While many questions remain over whether we can rely on notice of a company's privacy practices, and some, like Fred Cate note the costs and failures of notice,[34] it does remain a sound aspirational principle that must be transposed effectively.

The main shortcoming of this principle is that it contemplates that the work of notice will be done primarily, if not entirely, by "plain language statements about personal data collection, use, disclosure, and retention." While such statements *are* important and should be made more readable and conspicuous where feasible, as the FTC Report also proposes,[35] they should be supplemented in two key ways.

First, companies should be encouraged to educate consumers through more accessible forms of notice that explain privacy policies and practices, as the FTC Report contemplates. This could include short videos such as on Google's Privacy Channel on YouTube,[36] FAQs, just-in-time notices about how mobile apps collect data, and so on. The FTC should be commended for making this general inquiry the focus of its upcoming May Workshop.[37]

Second, the White House missed an opportunity to promote the concept of "Smart Disclosure" developed by Cass Sunstein, director of the Office of Information and Regulatory Affairs, a close advisor to the President, and a widely respected thinker in law, policy and technology. In an OIRA memo to agency heads issued last fall, Sunstein defined "smart disclosure" as:

> the timely release of complex information and data in standardized, machine readable formats in ways that enable consumers to make informed decisions. Smart disclosure will typically take the form of providing individual consumers of goods and services with direct access to relevant information and data sets. Such information might involve, for example, the range of costs associated with various products and services, including costs that might not otherwise be transparent. … In many cases, smart disclosure enables third parties to analyze, repackage, and reuse information to build tools that help individual consumers to make more informed choices in the marketplace.

This provides a powerful vision for reconceiving transparency as something that can be technologically intermediated—meaning that a company's disclosure of its privacy practices (among other things) need no longer be limited to the simplified form of its plain language

---

[34] "Businesses and other data users are burdened with legal obligations while individuals endure an onslaught of notices and opportunities for often limited choice. Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice." Cate, *supra* note 31, at 1.

[35] FTC Report at 61.

[36] The Google Privacy Channel, YouTube, http://www.youtube.com/googleprivacy

[37] Press Release, Federal Trade Commission, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012, Feb. 29, 2012, http://www.ftc.gov/opa/2012/02/dotcom.shtm.

disclosure (though, as discussed below, they should be consistent, or punished under the FTC's deception authority). Meaningful smart disclosure on privacy could bypass much of the current debate about the failure of effective notice to empower consumers by making "notice" technologically actionable: Users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app acedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct..

Further, as the FTC Report notes, "Machine-readable policies, icons, and other alternative forms of providing notice also show promise as tools to give consumers the ability to compare privacy practices among different companies."[38] Again, the example of an app store might illustrate how such comparisons could work, allowing users trying to choose between several competing apps to compare their privacy practices side by side.

The FTC Report contemplates a particular application that as Commissioner Brill put it in a public response to my question at a Direct Marketing Association event on the day the FTC Report was released, "... is the first step towards structured disclosure more generally."[39] Specifically, the FTC Report proposes that:

> the data broker industry explore the idea of creating a centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options. This website will improve transparency and give consumers control over the data practices of companies that maintain and share data about them for marketing purposes.[40]

This concept merits exploration as a way of remedying the lack of transparency regarding companies that currently lack a direct way of offering transparency to those whose data they collect—provided the term "data broker" is defined appropriately. This could be an excellent test case for encouraging smart disclosure through self-regulation—but only if it can be implemented in a way that actually improves transparency for consumers and proves feasible for companies.

---

[38] FTC Report at 62.

[39] Keynote Address by FTC Commissioner Julie Brill at DMA in DC 2012, March 26, 2012, http://newdma.org/dma-in-dc

[40] FTC Report at 69.

VII. Transposition of Principles

Setting aside the first question raised at the outset (choosing the right principles), the core problem remains a practical one: How to translate a set of principles (or "rights") into workable guidelines and, where appropriate, binding rules that inform how data flows across the Internet through countless interactions every minute and through technologies yet to be conceived.

The Report aptly summarizes the virtues of "open, transparent multistakeholder processes": "when appropriately structured, they can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges."[41] American reliance on multistakeholder processes has, as the Report notes, allowed the U.S. Internet policy to avoid "fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust."[42] (This essentially affirms what the FTC said in its 1999 report on privacy: "[S]elf-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[43])

But just as the value of privacy principles depends on their transposition into real-world guidelines, that process of transposition depends on whether it is "appropriately structured."[44] In both cases, what matters is not the intention, but the process, for the process is what determines the outcome. If we wish to avoid "failure by design," we must take care to answer the following critical questions carefully.

First, what role will government play? The White House Report says, "The Federal Government will work with stakeholders to establish operating procedures for an open, transparent process. Ultimately, however, the stakeholders themselves will control the process and its results."[45] Fulfilling this promise requires that, if government officials actually serve as facilitators for the process, they must remain neutral conveners, and the principles contained in the White House Report must be clearly understood as one set of hortatory principles, rather than criteria by which the success of the self-regulatory process *must* be judged.

This is the most important factor separating the kind of self-regulation praised by the White House and what the Europeans call "co-regulation." In self-regulation, government may suggest aspirational principles (as the White House has done) and play a convening role, but in co-regulation, government "steers while industry rows," steering the process to determine its outcome. Co-regulation is, in fact, just another vehicle for governmental regulation; and while it might seem comfortably familiar to European privacy regulators, it cannot be relied on to deliver the workable policy framework that can only be forged in a true self-regulatory process as a voluntarily agreed upon compromise among many stakeholders with conflicting interests.

---

[41] *Id*. at 23.

[42] *Id*. at 24.

[43] 1999 FTC Report at 6.

[44] White House Report at 24.

[45] *Id*. at 24.

While the experience of the Digital Advertising Alliance,[46] for example, is a great example of how a multi-stakeholder process can achieve industry consensus on a difficult set of issues, it verges on co-regulation in one key respect: This process is not a high-level framework such as that proposed by the White House Report, but a sector-specific set of principles for online behavioral advertising developed by the FTC.[47] However admirable the end result, the more specifically government sets the basic contours of the self-regulatory process, the more likely that process is to produce outcomes that prove unworkable to some in industry.

Indeed, the less the multistakeholder process verges on co-regulation, the lower the risk of another failure point in the self-regulatory process: a legal challenge by a company that the process constituted government action that should have been subject to normal rulemaking requirements, or that it exceeded the jurisdiction of whichever agency might run the process.

Second, just how "open" and "transparent" must the process be? Requiring all discussions to take place in public would chill the very open dialogue among companies about their technologies and business practices necessary to allow self-regulation to distill widely dispersed expertise into workable compromises. This reality demands that at least some negotiations be conducted in private, without government or privacy advocates in the room—because both could use information derived from these negotiations in litigation against (or at least public criticism of) particular companies, something that would chill candid participation by those companies.

Third, how will civil society groups participate in the process? If they may exercise a "heckler's veto," they could derail the process. On the other hand, they may prove invaluable to the success of the process so long as their criticism is constructive, offering concrete suggestions on how to better protect privacy. And to the extent they can support the codes of conduct that result from the process, or at least the legitimacy of the process that produced them, the evolving U.S. privacy regime will benefit from greater acceptance by the public and our International partners. Of course, they need not accept these codes as the final word on the matter, and remain free to produce their own "minority report" or lobby for legislation in a particular area.

The model of the Digital Advertising Alliance is thus further instructive: Industry responded to the problem identified by the FTC's 2009 “Self-Regulatory Principles For Online Behavioral Advertising” by convening their own multi-stakeholder process behind closed doors, resulting in a set of principles unanimously approved by the participating companies.[48] The DAA published a draft report, solicited feedback from privacy advocates and the FTC, and reconvened their process to produce a final code of conduct, to which they unanimously certified.

---

[46] Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data* (2011), http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[47] Federal Trade Commission, *Self-Regulatory Principles for Online Behavioral Advertising* (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[48] Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* (2009), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

Fourth, by whom will self-regulatory codes of conduct be subject to approval? The White House Report merely says "the stakeholders themselves will control the process and its results"[49] but does not clarify what that means. Outrageous as it will surely seem to some, it must be industry itself that determines whether to approve a code of conduct. Otherwise, the process will fail because companies simply will not abide by the codes of conduct it produces. This is likely to be the most controversial aspect of designing the multi-stakeholder process because the expectations of privacy advocates are simply unrealistic. For example, in testimony before this Subcommittee last October, Pam Dixon of the World Privacy Forum demanded "Consumer, public interest and other independent representatives must be fully represented (if possible, up to 75 percent or more) on the governing bodies of self-regulatory schemes."[50]

Given such expectations, not getting to vote *at all* on approval will be a difficult pill for many well-meaning privacy advocates to swallow. But they can still meaningfully shape the outcome of these self-regulatory processes even without voting on the final product, not only through their official input in the process, but through their ability to channel public pressure on the companies that participate. The widespread public opposition to SOPA and PIPA earlier this year demonstrated just how powerful public pressure can be. There is no reason why civil society groups cannot attempt to use such grassroots pressure to influence the self-regulatory process.

Fifth, regardless of *who* votes, what will be the mechanism for voting? How high will the threshold be for approval, and how will voting power be determined? These are questions best answered by professionals with expertise in designing choice mechanisms for multi-stakeholder processes. As a number of economists have shown, the outcomes of a voting system are highly contingent on its structure.[51] Commissioner Rosch's concern about the danger of capture by industry leaders is worth noting.[52] But it nonetheless seems inevitable that voting power will have to be related in some fashion to market share. Otherwise, the outcome will be determined by who can get more seats at the table—much as the Soviet Union once tried to increase its representation in the United Nations by insisting that Soviet Republics like Byelorussia and Ukraine deserved their own seats.[53]

---

[49] White House Report at 24.

[50] Testimony of Pam Dixon, Executive Director, World Privacy Forum, Before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, Oct. 13, 2011, at 11, http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/101311/Dixon.pdf.

[51] James Buchanan & Gordon Tullock, *The Calculus of Consent: Logical Foundations of Constitutional Democracy*, http://www.econlib.org/library/Buchanan/buchCv3.html.

[52] "[T]he self-regulation that is championed in this area may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power. That possibility may be blunted by insuring that smaller rivals participate in the adoption of self-regulatory rules, but that may not be practical." Rosch statement, 2010 Draft Privacy Report at E-3.

[53] *See* N.S. Timasheff, *Legal Aspects of the Grant of Three Seats to Russia in the United Nations Charter*, 14 Fordham L. Rev. 180 (1945), http://ir.lawnet.fordham.edu/flr/vol14/iss2/4.

Sixth, will there be a shot clock for the process? If so, how will it work? If not, how can we ensure that each self-regulatory process work expeditiously and that those companies that prove resistant to compromise will not unduly drag out the process as a negotiating tactic? As with the voting mechanism, reasonable time limitations that are made clearly *ex ante* can help to avoid process failure—so long as they provide adequate time to resolve the issues specific to that process.

Seventh, how will the initial selection of issues work? The White House Report proposes only that "Stakeholder groups, with the assistance of NTIA, will identify markets and industry sectors that involve significant consumer data privacy issues and may be ripe for an enforceable code of conduct."[54] This conversation is probably one that can happen entirely in public, and would very much benefit from the active (and constructive) participation of civil society groups. The best way to approach this process may be to create a prioritized list of issues that make sense of the basis for a potential code of conduct, either specific to an industry or to a cluster of related practices.

For example, early topics to be considered might include transparency in the mobile ecosystem (a topic on which the FTC will hold a workshop in May[55]), cross-border transfers of cloud data, and transparency regarding "data brokers" whose operations are not directly visible to the public (a topic identified as critical by the FTC Report—but without any definition of the broad term "data broker"[56]). Other topics that may merit attention include the portability of user data, interoperability of privacy controls, and machine-readable disclosures (discussed above).

Finally, how exactly will self-regulatory codes of conduct be updated? By shaping expectations during initial negotiation, this question will play a large role in the success or failure of the initial process. The White House Report raises as many questions as it answers in this regard with its discussion of "evolution": "Stakeholders may decide at any time that a code of conduct no longer provides effective consumer data privacy protections, in light of technological or market changes."[57] How many? Much like the initial voting mechanism question, industry participants need to know *ex ante* what will be required to re-open negotiation of, and actually amend, a code of conduct. This is probably a question best resolved by industry itself in the initial negotiations. "NTIA might also … seek to re-convene stakeholders. As with the initial development of a code of conduct, however, stakeholder participation in the process to revise a code of conduct would be voluntary."[58] So what will constitute an effective "quorum" for a revised process? Or will it be sufficient that some companies might accede to a version 2.0 of a code? What will happen if a code "forks" into multiple pieces (as sometimes happens with

---

[54] White House Report at 26.

[55] Press Release, Federal Trade Commission, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012, Feb. 29, 2012, http://www.ftc.gov/opa/2012/02/dotcom.shtm.

[56] FTC Staff Report at 68-70.

[57] White House Report at 27.

[58] *Id.*

open source standards)? If "Congress could prescribe a renewal period for codes of conduct," what would be required to renew and extend them?

VIII. Accountability: Effective Enforcement

Having discussed the first and second questions identified at the start of this testimony, let us now turn to the third: how the FTC can effectively enforce compliance. This has three component parts:

- Institutional enforcement capacity
- Deception authority
- Unfairness authority

The White House Report rightly emphasizes the need for "strong enforcement," but focuses on granting new legal authority to the FTC. Before reaching this point, the Report should have asked whether the FTC has the enforcement capacity necessary to use its existing authority—or to use any new authority it might be given—and whether that existing legal authority is being fully realized.

A. Enforcement by the Reputation Market

But before turning to turning enforcement by government, it is worth considering the way the Internet itself facilitates pressure on companies through the "reputation market" to abide by their privacy promises and improve their privacy practices. The social media revolution has made it possible for anyone concerned about online privacy to blow the whistle on true privacy violations. That whistle may not always be loud enough to be heard, but it's more likely to in this sector than any other. Traditional media sources like the Wall Street Journal have played a critical role in attracting attention to corporate privacy policies through its "What They Know" series,[59] which has been popularized using social media tools.

Social media tools were recently used to great effect to express grassroots concern about proposed copyright legislation. While some Internet companies certainly helped to promote these messages, even without their involvement, this experience demonstrates how effective social media activism can be. There is no reason why such techniques cannot be used effectively against major Internet companies themselves, just as Facebook users have used Facebook itself to rally opposition to Facebook on privacy concerns such as its Beacon ad targeting system.[60] Among the most important factors driving companies to participate

---

[59] *What They Know,* Wall St. J., 2012, http://blogs.wsj.com/wtk/.

[60] See, e.g., Kirsten E. Marti, Facebook (A): Beacon and Privacy 3 (2010), *available at* http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf ("The online community responded immediately to this intrusion. MoveOn.org created a Facebook group —Petition: Facebook, stop invading my privacy that stated: —Sites like Facebook must respect my privacy. They should not tell my friends what I buy on other sites—or let companies use my name to endorse their products—without my explicit permission The Facebook group and petition had 2,000 members within the first 24 hours and eventually grew to over 80,000 names.").

constructively in the multi-stakeholder process, to forge meaningful privacy protections, and to abide by them will be the fear of a Wall Street Journal article, a social media frenzy, or organized campaign demanding action on a particular privacy problem.

B. Enhancing the FTC's Institutional Technical Capacity

Effective FTC enforcement requires the technical knowledge of the industry. Chairman Leibowitz deserves credit for appointing the agency's first Chief Technologist.[61] But even with someone as talented as Ed Felten in that position, the FTC is still way behind the curve: Ed's title is not Chief Technology *Officer* because there is no office behind him. Just over five years ago, Peter Swire called on the agency to "consider a new office of information technology to assist the Commission in making effective decisions about how to protect consumers in Internet activities. This office would parallel the FTC's in-house capability in economics, and would permit the FTC to act strategically to protect consumers from emerging online threats."[62]

Specifically, the Report should have called for a clear strategic plan outlining (a) how to build the in-house technical expertise it needs (beyond basic IT infrastructure) to identify enforcement actions, support successful litigation, monitor compliance, and conduct long-term planning and policy work, and (b) the resources necessary to achieve that goal through a combination of re-prioritizing current agency spending and additional appropriations. Importantly, this organization should function as a cohesive team that meets the needs for technical expertise of all the FTC's bureaus and offices (including the Bureau of Competition). A stand-alone organization could, like the Bureau of Economics, better attract and retain talent.

These suggestions in no way diminish the important enforcement work done by the FTC's hardworking staff. To the contrary, it is unfair and unrealistic to expect the FTC to fulfill its consumer protection mission in the face of massive technological change without the expertise required to stay ahead of that change. If, in the last five years, policymakers had spent a fraction as much time on improving the FTC's institutional capacity as inventing new authority, the U.S. privacy regime would be far more effective in protecting consumers and ensuring their trust, and less easily dismissed as inadequate by foreign privacy regulators.

C. Enhancing the FTC's Deception Authority through Smart Disclosure

Punishing deception is the bedrock of the FTC's current privacy regime[63]—and it will the the ultimate tool for ensuring accountability by companies to the self-regulatory codes of conduct to which they subject themselves. Yet both the White House Report and the FTC Report miss

---

[61] Federal Trade Commission, *FTC Names Edward W. Felten as Agency's Chief Technologist; Eileen Harrington as Executive Director*, Nov. 4, 2010, http://www.ftc.gov/opa/2010/11/cted.shtm.

[62] Peter Swire, *Funding the FTC: Globalization and New Information Technologies Necessitate an Appropriations Boost*, February 26, 2007, http://www.americanprogress.org/issues/2007/02/ftc.html

[63] "[T]he Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." FTC Policy Statement on Deception, 1983, http://www.ftc.gov/bcp/policystmt/ad-decept.htm (appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984)).

an important opportunity to enhance the FTC's deception authority through the enforcement of structured, machine-readable disclosures.

At a minimum, such disclosures could be used to indicate which self-regulatory codes of conduct the site or service complies with. This, in turn, should facilitate FTC enforcement by allowing the agency to easily determine the universe of companies acceding to the code.

In a more robust form, machine-readable disclosures could also be used by companies that want to accede to most of a code of conduct but not to particular components of its rules—or all of a code, *plus* additional protections. This might create a practicable way of managing enforcement of a multiplicity of codes of conduct without requiring binary all-or-nothing compliance. That, in turn, might help to facilitate both successful resolution of the multistakeholder process and continuing competition on privacy. In other words, companies are more likely to treat codes of conduct as a floor for their practices, rather than a ceiling, if they can be rewarded for exceeding the basic requirement of a code.

But to succeed in promoting the White House's Accountability principle, smart disclosures must be as legally enforceable as the plain language versions to which they correspond. The Deception Doctrine requires that a misrepresentation or omission be both likely to mislead a consumer and "material."[64] Thus, for example, a machine-readable statement about corporate privacy practices that was implemented as an industry standard but never adopted in any way that consumers actually relied upon might not be subject to a deception action, no matter how misleading a disclosure in that format might be. On the other hand, once relied upon by even a relatively small group of consumers, such a disclosure system *should* be legally enforceable under the Deception Policy Statement, which specifically notes that, "If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group."[65] In other words, even if only a relatively niche group of "power users" used a setting in their app store to limit installations to apps that complied with certain privacy practices, or acceded to particular codes, these representations should be enforceable by the FTC.

Unfortunately, such case of widespread deception has persisted for many years without an FTC enforcement action. In 2002, W3C published P3P: The Platform for Privacy Preferences,[66] which allows websites to describe their privacy practices in a compact privacy policy. Internet Explorer, starting with version 6 (released in 2001), will, by default, not load third party cookies from sites that do not have a compact privacy policy.[67] It was widely known for many years that many companies created compact privacy policies that did not correspond to their human-readable privacy policy (or their actual privacy practices), but in 2008 Lorrie Faith Cranor

---

[64] *Id.*

[65] *Id.*

[66] Platform for Privacy Preferences (P3P) Project, Enabling Smarter Privacy Tools for the Web (2007), http://www.w3.org/P3P/.

[67] Privacy in Microsoft Internet Explorer 6, MSDN, http://msdn.microsoft.com/en-us/library/ms537343.aspx

published a research paper documenting widespread mis-statements in P3P policies.[68] In December, a federal court dismissed a suit against Amazon on similar grounds for lack of standing,[69] making it clear that if P3P policies are to be enforced, the task must fall to the FTC.

While the FTC has never, to my knowledge, explained why it has not brought an enforcement case based on P3P misrepresentations, one possible explanation is that they have concluded that the IE6 implementation is inadequate to demonstrate that the representations within the compact privacy actually mislead consumers, as the Deception Policy Statement requires, because IE6 requires only that a site have a policy, not that the policy say anything in particular.

If so, the lesson is that any self-regulatory effort geared toward using machine-readable disclosures should be conducted in conjunction with those who might develop tools based on such disclosures, particularly browser-makers, to ensure that the useful disclosures are implemented by useful tools.

D. Using the FTC's Unfairness Authority

The FTC's unfairness jurisdiction is often mentioned only as an afterthought, but in fact, as the Commission has held, "unfairness is the set of general principles of which deception is a particularly well-established and streamlined subset."[70] As so often happens in policy discussions, the Report pays scant attention to the FTC's unfairness jurisdiction, merely noting, in a footnote, that it "will remain an important source of consumer data privacy protection."[71] In fact, this jurisdiction is the key to how the FTC could effectively police online privacy outside of self-regulation—punishing companies that do not participate in self-regulation as well as practices that are not prohibited by self-regulation.

This jurisdiction is a powerful tool against privacy abuses because it allows the FTC to build a quasi-common law limiting harmful trade practices as technology evolves. But unfairness can

---

[68] Lorrie Faith Cranor, Serge Egelman, Steve Sheng, Aleecia M. McDonald & Abdur Chowdhury, *P3P Deployment on Websites*, 7 Electronic Commerce Research and Applications 3, 274-293 (Autumn 2008), *pre-print available at* http://lorrie.cranor.org/pubs/p3p-deployment.html (In a study comparing the actual P3P policies of 21 popular websites to the corresponding natural language policies, the researchers found that only two P3P policies correctly specified the types of data that were being collected. As a result, "users reading only a P3P policy might be surprised to find a site collecting more data than what was advertised." p. 40. All of the sites has discrepancies regarding the ways in which collected data may be used. p. 40-41. And "[o]nly six of the websites examined either accurately report their data sharing policies ... or their P3P policies are overly inclusive ... in their reporting of data sharing." p. 41.).

[69] Del Vecchio v. Amazon, C11-366-RSL (W.D. Wash.; Dec. 1, 2011), available at http://docs.justia.com/cases/federal/district-courts/washington/wawdce/2:2011cv00366/174037/58/0.pdf?ts=1322842930; *see also* Venkat Balasubramani, *The Cookie Crumbles for Amazon Privacy Plaintiffs – Del Vecchio v. Amazon*, Technology & Marketing L. Blog, Dec. 2, 2011, http://blog.ericgoldman.org/archives/2011/12/the_cookie_crum.htm.

[70] International Harvester, 104 F.T.C. 949, 1060 (1984) *(cited in* J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, § III, http://www.ftc.gov/speeches/beales/unfair0603.shtm [hereinafter *Beales Paper*]).

[71] Report at 27 note 32.

be a dangerous legal weapon if unleashed from its current limitations. Understanding the checkered history of the Unfairness Doctrine is essential to understanding the evolution of the FTC and U.S. consumer protection law more generally. In brief, until 1964, the agency generally did not distinguish between unfair acts and deceptive ones. In 1964, the agency defined "unfairness" in highly subjective terms, without weighing the benefits of a practice or how easily consumers could avoid it.[72] This led the FTC on an unfairness rule-making spree, trying to regulate everything from funeral home practices to advertising to children—to the point that it was dubbed the "National Nanny" by the Washington Post—hardly a Thatcherite bastion.[73] In fact, the Democratic Congress responded by briefly shutting down the agency and slashing its budget to make it clear that it had not dubbed the agency a regulatory knight errant, free to tilt its steely lance at imagined windmills of "unfairness" or "deception."[74] While this experience did serious harm to the FTC's institutional capacity,[75] it also led to the formulation of clear policy statements on unfairness (in 1980) and deception (in 1983), both at the request of Congress. These today provide the basis for the FTC's enforcement actions, and also reasonably clear legal standards by which companies may predict their legal liability. In 1994, Congress enshrined the Unfairness Policy Statement in the FTC Act itself.[76]

Under the Statement and the 1994 amendment, the Commission applies a two part test. First, it asks whether an "unjustified consumer injury" has occurred:

> To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.[77]

Second, the FTC will consider:

> whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise. This criterion may be applied in two different ways. It may be used to test the validity and strength of the

---

[72] See generally, Beales Paper, *supra* note 70.

[73] *Id.* (*citing* Wash. Post, March 1, 1978).

[74] *Id*.

[75] The agency in 2010 had 34% fewer full time equivalent employees as it did in 1980 (even without adjusting to for the growth in U.S. population)—and that number has grown significantly since the original slashing. *See* FTC Full-Time Equivalent History, http://www.ftc.gov/ftc/oed/fmo/fte2.shtm.

[76] 15 U.S.C. § 45(n) ("The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

[77] 1980 FTC Unfairness Policy Statement.

> evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present.[78]

But, by statute, "[s]uch public policy considerations may not serve as a primary basis for such determination."[79] Howard Beales has summarized the Unfairness Doctrine as follows:

> the modern unfairness test reflects several common sense principles about the appropriate role for the Commission in the marketplace. First, the Commission's role is to promote consumer choices, not second-guess those choices. That's the point of the reasonable avoidance test. Second, the Commission should not be in the business of trying to second guess market outcomes when the benefits and costs of a policy are very closely balanced or when the existence of consumer injury is itself disputed. That's the point of the substantial injury test. And the Commission should not be in the business of making essentially political choices about which public policies it wants to pursue. That is the point of codifying the limited role of public policy.[80]

The FTC has used its unfairness authority to protect privacy in several lines of cases. First, as noted in the FTC's 2010 Preliminary Staff Report, the Commission brought a number of unfairness cases requiring adequate security practices.[81] But as Commissioner Rosch noted in his concurring statement, "there was financial harm threatened in those cases."[82] Second, the FTC has brought unfairness actions to punish retroactive application of a revised privacy policy.[83] Third, late last year, the FTC brought, and successfully settled (but did not fully litigate) an unfairness case against Frostwire, the maker of a mobile peer-to-peer file-sharing program for its unfair product design. This case is groundbreaking both because it applies unfairness in the context of how product design can cause users to share more information than they expect and because it rests on non-monetary harms.

E. Unfairness and the Harm Debate

As noted above, the extent of the Unfairness Doctrine's applicability rests primarily on how broadly harm is defined—as is implied by the FTC's declaration that "Unjustified consumer injury is the primary focus of the FTC Act.""[84]

---

78 *Id.*

79 15 U.S.C. § 45(n).

80 Beales Paper, *supra* note 70.

81 2010 FTC Report at 10.

82 2010 FTC Report at E-2 n. 3.

83 See, e.g., Gateway Learning Corp., No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/0423047.shtm; Federal Trade Commission, *Self-Regulatory Principles for Online Behavioral Advertising supra* note 47, at 19; *see also* In re Orkin Exterminating Co., 108 F.T.C. 263 (1986), aff'd, 849 F.2d 1354 (11th Cir.).

84 1983 FTC Unfairness Policy Statement.

Even critics of the Unfairness Doctrine have been careful not to rule out its proper application in privacy cases. For example, in 2000, the Commission settled an enforcement action against ReverseAuction, which had violated eBay's terms of service by "using the e-mail addresses, eBay user IDs, and feedback ratings of eBay registered users for the purposes of sending unsolicited commercial e-mail to such registered eBay users."[85] Commissioners Swindell & Leary dissented, in part, on the grounds that this should have been a pure deception case and that violating user privacy by sending such unsolicited email "did not cause substantial enough injury to meet the statutory standard" but emphasized that "[w]e do not say that privacy concerns can never support an unfairness claim." Instead, they simply argued that: "This standard for substantial injury overstates the appropriate level of government-enforced privacy protection on the Internet, and provides no rationale for when unsolicited commercial e-mail is unfair and when it is not. We are troubled by the possibility of an expansive and unwarranted use of the Unfairness Doctrine."[86]

Howard Beales, former Director of the FTC's Bureau of Competition, argues that "Subjective value, as opposed to emotional distress, can be a form of real injury. For example, falsely claiming that a product is kosher would cause real harm to anyone on a kosher diet."[87] More importantly, he argues that reputational harm can be "substantial injury" under the Unfairness Doctrine. In a 2003 case brought by the Bureau of Competition under Beales, the FTC successfully settled a spoofing case:

> "Spoofing" is the practice of making it appear that bulk, unsolicited commercial e-mail ("spam") comes from a third party to the transaction by placing that person or entity's e-mail address in the "from" line of the spam. As a result... spoofing portrays these innocent bystanders as duplicitous spammers, often resulting in their receiving hundreds of angry e-mails from those who had been spammed.
>
> The Commission alleged that this practice was unfair in a federal district court complaint against Brian Westby, who used spam to direct traffic to an adult website. The spam also contained deception in the subject line, tricking consumers, including children, into opening the e-mail and being subjected, in some cases, to graphic adult images. The Commission alleged that this was deceptive. The deception theory, however, does not provide any relief to those consumers who were "spoofed," because they have not relied in any way upon Westby's deception. Unfairness, however, easily reaches the problem. The harm to those consumers - both economic injury caused by damage to their computing

---

[85] Complaint, FTC v. ReverseAuction.com, Inc. File No. 0023046, (Jan. 6, 2000), available at http://www.ftc.gov/os/2000/01/reversecmp.htm.

[86] Statement of Commissioners Orson Swindle & Thomas B. Leary, FTC v. ReverseAuction.com, Inc., File No. 0023046, (Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversesl.htm.

[87] Beales Paper, *supra* note 70 (citing Timothy J. Muris, *Cost of Completion or Diminution in Market Value: The Relevance of Subjective Value*, 12 J. Legal Stud. 379 (1983)).

> systems by the huge, unexpected influx of mail, the time spent deleting thousands of e-mails, and *the injury to reputation of having their name associated with deceptive adult spam - is substantial*. Hiding the real spammer's identity has no benefit to consumers or competition, so the amount of injury, though substantial, need not be high. Finally, there is no way consumers can anticipate and protect themselves from such an invasion. Anyone with an e-mail account is vulnerable.[88]

In the *Frostwire* case, the FTC alleged a number of non-monetary harms:

> Public exposure of the types of user-originated files that FrostWire for Android shared following a default installation and set-up could increase consumers' vulnerability to identity theft; *reduce their ability to control the dissemination of personal or proprietary information* (e.g., voice recordings or intimate photographs); and increase their risk of legal liability based on prohibitions against, or limitations on, making any such files publicly available for download.[89]

In short, the FTC has staked out a bolder position on the scope of harm covered by unfairness than many realize. This is not, to be sure, the end of the debate. Since these cases have not been litigated, but rather settled before full litigation, it is not certain that this position would survive completely in court. And, on the other hand, FTC Commissioner Julie Brill has raised some difficult questions about the need to recognize harms that are probably more amorphous than ought properly to be recognized under the Unfairness Doctrine.[90]

But as noted at the outset, harms not covered by the Unfairness Doctrine should be addressed by Congress, if at all, under the basic analysis of the Unfairness Doctrine: weigh consumer harm against consumer benefit and intervene only where consumers themselves cannot reasonably avoid the harm, such as through more effective privacy controls. Congress might eventually choose to deem certain practices injurious so that the FTC will need to apply only the other elements of the test. The Unfairness Doctrine contemplates such action through its second prong, clearly established public policy.

The FTC can, however, help to clarify this uncertainty by convening a public workshop on its unfairness authority, with a special emphasis on what it considers the proper definition of harm. Ideally, such a workshop would produce guidelines building on the 1980 Unfairness Policy Statement adequate to help companies predict how to build new and innovative services without running afoul of the unfairness authority. If the FTC pushes the boundaries of harm

---

[88] Beales Paper, *supra* note 70*; See also* FTC v. Westby, No. 03-C-2540 (N.D. Ill. 2003), http://www.ftc.gov/os/2003/09/marriedcomp.pdf.

[89] F.T.C. v. Frostwire L.L.C., No. 11-23643-CV-GRAHAM (S.D. Fla. 2011), at 17. The last claim appears to refer to, *inter alia*, legal restrictions on, for example, making photographs of others publicly available without their consent.

[90] FTC Commissioner Julie Brill, *Big Data, Big Issues*, Remarks at Fordham University School of Law (Mar. 2, 2012), http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

too far, Congress should intervene, as it did when it ordered the FTC to prepare its policy statements on unfairness and deception in the early 1980s.

F. The Use of Unfairness Authority to Supplement Self-Regulation

While self-regulation does not constitute established public policy adequate to justify an unfairness action on its own (if violated by a company that never acceded to a voluntary code of conduct, therefore making a deception action impossible), self-regulation may *indirectly* bolster an unfairness action—as the *Frostwire* case implies. This nuanced distinction is important to fulfilling the White House Report's promise that "There is no Federal regulation at the end of the process, and codes will not bind any companies unless they choose to adopt them."[91]

Prior to 1983, the Commission considered industry practice as well as statutes and the common law in determining whether a practice violated public policy. But the 1983 Unfairness Policy Statement implies that industry practice may play only a limited role in determining whether a practice violates public policy.[92] The 1994 amendment to the FTC Act goes a step further and declares that "public policy considerations may not serve as a primary basis for [an unfairness] determination."[93] Thus, the precise significance of industry practice remains somewhat unclear—a question that merits clarification by the FTC.

This means that industry practice, such as might be established through self-regulation, will primarily influence the consumer injury prong of unfairness, which the FTC has called "the primary focus of the FTC Act," and which can, "by itself it can be sufficient to warrant a finding of unfairness."[94]

Specifically, in the *Frostwire* case settled late last year, the FTC's unfairness argument relied, in significant part, on the fact that it was not standard industry practice to "allow the public disclosure of private files by default"[95] in establishing two of the three prongs required by the FTC's 1980 Unfairness Policy Statement. Under the third prong, the FTC argued that "a significant number of consumers using Frostwire for Android could not reasonably avoid the unwitting public sharing of their private files. These consumers would not have understood that FrostWire for Android operated in the manner described above from either the Defendants' disclosures or from prior experience with other software."[96] Under the second prong, the FTC argued that "the design and default settings [of Frostwire for Android] provided

---

[91] *Id*. at 24.

[92] 1983 FTC Unfairness Policy Statement ("To the extent that the Commission relies heavily on public policy to support a finding of unfairness, the policy should be clear and well-established. In other words, the policy should be declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values.").

[93] 15 U.S.C. § 45(n)

[94] 1983 FTC Unfairness Policy Statement.

[95] *Frostwire Complaint* at 17.

[96] *Id.* at 16.

few or no countervailing benefits to consumers or competition. Configuring software applications to allow the public disclosure of private files by default runs counter to standard software development guidance, and counter to established practices in the development of file-sharing applications."[97]

It would, of course, have been better—from the perspective of crafting predictable legal standards—if a court had weighed such arguments in an adversarial proceeding and provided guidance on where, exactly, to draw the line on both counts. But both arguments would likely have prevailed in court, had the FTC not settled the case. In this sense, such settled complaints form the basis of a quasi-common law of unfairness (or deception) that is at least adequate to allow companies wrestling with technological change to predict with reasonable confidence what the FTC is likely to consider a violation of Section V of the FTC Act.

The FTC's first argument hinges on their claim that "Nothing in the FrostWire for Android installation and set-up process, or the application's user interface, adequately informed consumers that the application operated in this manner."[98] In this context, the inconsistency of a practice (in this case, public disclosure of private files by default from a peer-to-peer mobile application) with standard industry practice speaks to whether it would have occurred to the reasonable consumer to investigate (a) which files the software made publicly available and (b) how to change the default setting. Simply put, the failure of transparency makes industry standards more dispositive of whether consumers would rightly expect a harmful practice.

The FTC's second argument—that industry standard for software design bear on the analysis of countervailing benefits to consumers or competition—seems somewhat more tenuous but still convincing in this case. While the FTC did not elaborate on this point (as it would have had to do before a judge had the case not been settled), it seems reasonable to argue that compliance with industry standards can benefit consumers both by lowering product design costs and also by lowering the non-monetary costs to users of learning and using a particular product interface. This is not to say that non-compliance with such standards is itself a harm, but it certainly is not a benefit if the non-compliant user interface shares sensitive information by default and makes it extremely difficult for consumers to realize this and change the necessary setting. Of course, more important than this lack of benefit is that the default sharing setting in this case did not seem to provide users a "countervailing" benefit sufficient to outweigh the potential harm flowing from the inadvertent disclosure of all the files on a user's Android device.

In summary, the *Frostwire* case does *not* stand for the proposition that industry self-regulation necessarily binds non-participating companies in its prohibitions on specific practices, but rather for the proposition that, if a company engages in a practice that diverges from industry practice *and* meets the other required elements of unfairness (causing a "substantial injury" that is "not be outweighed by any countervailing benefits to consumers or competition"), its

---

[97] *Id.*at 17.

[98] *Id.*at 16.

burden of empowering consumers to avoid that practice grows as the degree of divergence of industry practice increases.[99] Thus, the Unfairness Doctrine already offers the FTC a tool for implementing the second prong of the new framework it proposes in the FTC [Draft] Report: "For data practices that are not 'commonly accepted,' consumers should be able to make informed and meaningful choices."[100]

Concretely, then, *Frostwire* means that at least some companies that choose not to accede to the standards established by the self-regulatory process envisioned by the White House Report may have to engage in a heightened degree of "Privacy by Design" planning to analyze their non-compliant privacy practices under an unfairness analysis. Depending on their analysis of consumer harms and benefits, they may feel obliged to build accordingly more robust, and more usable, user interfaces that inform the consumer as to privacy defaults and how to change them.

This is precisely as it should be: Using its unfairness authority, the FTC can thus build on self-regulation *without* forcing compliance with self-regulation—in which case self-regulation, no matter how "voluntary" at its outset, would become co-regulation: just another vehicle for imposing top-down solutions on a complex ecosystem that requires, as the Report notes, the "flexibility, speed, and decentralization" that only true self-regulation can provide.

Yet the self-regulatory process is no less voluntary because companies that do not sign on to self-regulatory codes of conduct may be subject to somewhat elevated risks of unfairness enforcement actions for practices that diverge from industry practices established through self-regulation. But it *is* important that industry understand that the FTC's unfairness authority may play an increasingly important role as the U.S. privacy regime evolves towards more robust self-regulation. In this sense, it is that much more unfortunate that neither the White House Report nor the FTC Report does more to explain this seemingly esoteric and under-used, but extremely important, area of law. The FTC workshop and guidelines on unfairness proposed above should specifically consider how unfairness might apply to non-compliance with self-regulatory codes of conduct.

G. Self-Regulatory Policing

Robust self-regulation should involve industry enforcing the requirements on its own—in addition to FTC enforcement. The Digital Advertising Alliance has coordinated with the Better Business Bureau on just such a self-regulatory enforcement program.[101] If successful in demonstrating compliance and/or bringing enforcement actions against non-compliant companies, this enforcement program could be a model for other self-regulatory enforcement programs.

---

[99] This responsibility would, of course, also grow in proportion to the substantiality of the injury that could result from that practice, and in inverse proportion to the benefits from the practice.

[100] 2010 FTC Report at vi; *see also id*. at 40.

[101] Jack Marshall, DAA Steps Up Enforcement of Self-Regulatory Program, May 23, 2011, http://www.clickz.com/clickz/news/2073203/daa-steps-enforcement-self-regulatory-program

H. Private Ordering through Contract

Just as the White House Report acknowledges the importance of self-regulation, it also recognizes the critical importance of private ordering through contract to ensuring effective enforcement of privacy rules. Under the principle of Individual Control:

> When consumer-facing companies contract with third parties that gather personal data directly from consumers (as is the case with much online advertising), they should be diligent in inquiring about how those third parties use personal data and whether they provide consumers with appropriate choices about collection, use,and disclosure.[102]

And under the Accountability principle:

> Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise. … if a company transfers personal data to a third party, it remains accountable and thus should hold the recipient accountable—through contracts or other legally enforceable instruments—for using and disclosing the data in ways that are consistent with the Consumer Privacy Bill of Rights.[103]

Structured disclosures could help to promote compliance with such principles by making it more immediately evident (and potentially searchable) whether a company's partners abide by at least the same privacy protections. Or, structured disclosures could be used to identify who a company's partners are and directly link to their privacy policies.

IX. Privacy Regulation as International Trade Barrier

A final word about enforcement: selective enforcement may be a tool for invidious discrimination by national privacy regulators, most notably by European Data Protection Authorities against American companies. Yet neither the White House Report nor the FTC Report discuss the ways discriminatory enforcement of privacy laws against American companies burden international trade in data and the products and services enabled by data—or how to ensure that our own regulations do not do the same to foreign companies. In fact, the Administration has already recognized that privacy protections, however well-intentioned can, in fact, function as barriers to international trade. At last September's APEC meeting, U.S. Ambassador Phillip Verveer warned that privacy regulations that could slow adoption of cloud services:

> In these circumstances, we would expect every economy to welcome cloud services without regard to the national origin of their producers. But there are

[102] White House Report at 11

[103] *Id.* at 21.

> complications. One of the big ones is the limitations on trans-border data flows …. It is very important, however, that we not unnecessarily sacrifice the economic advantages inherent in cloud computing in our arrangements to protect personal privacy. Stated more directly, we should not let our quest for effective privacy mechanisms become a barrier to international trade in cloud services.[104]

This concept requires further conceptual development but it certainly deserves more attention.[105] It could also be the subject of a very productive workshop, perhaps convened by the Commerce Department.

[104] Patrick Ryan, *Cloud Services and International Trade*, Google Enterprise Blog, (Oct. 13, 2011), http://googleenterprise.blogspot.com/2011/10/cloud-services-and-international-trade.html.

[105] *See generally*, Bob Boorstin, *Promoting Free Trade for the Internet Economy*, Google Pub. Pol'y Blog (Nov. 15, 2010), http://googlepublicpolicy.blogspot.com/2010/11/promoting-free-trade-for-internet.html.

TECH FREEDOM

Responses to Questions for the Record of
Berin Szoka
President, TechFreedom[1]
on
Balancing Privacy and Innovation:
Does the President's Proposal Tip the Scale?

Hearing of the Subcommittee on Commerce, Manufacturing, and Trade
Energy & Commerce Committee
United States House of Representatives

March 29, 2012[2]

The Honorable Mary Bono Mack

1. You suggested that before granting the FTC new authority in the privacy arena, Congress should wait to learn from the self-regulatory process. By its nature, it may take quite a while before that process plays out fully. What should happen in the meantime?

My recent testimony before the Senate Commerce Committee[3] expanded upon my testimony before your committee. Congress should focus on enhancing the existing legal framework as a more resilient approach to privacy concerns than enacting "baseline" legislation in six ways:

1. Ensure the FTC has adequate institutional resources and expertise.
2. Require the FTC to explain how it has applied its baseline doctrines of consumer protection—deception and unfairness—in past privacy cases. A retrospective analysis in the form of guidelines analogous to the Antitrust Guidelines issued jointly by the FTC

---

1 Berin Szoka (bszoka@techfreedom.org, @BerinSzoka) is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on consumer privacy. In particular, he has testified on privacy and the self-regulatory process before the House Energy & Commerce Committee on March 29, 2012, available at http://tch.fm/KCrz8k ("Szoka Testimony I"),and the Senate Commerce Committee on June 28, 2012, available at http://techfreedom.org/sites/default/files/Szoka%20Testimony%20at%20Senate%20Privacy%20Self-Regulation%20Hearing%20v2.pdf ("Szoka Testimony II").

2 Available at http://energycommerce.house.gov/hearing/balancing-privacy-and-innovation-does-presidents-proposal-tip-scale

3 *See* Szoka Testimony II, *supra* note 1.

and Department of Justice[4] would serve two ends: (1) making the future course of the FTC's quasi-common law of privacy more predictable and (2) identifying areas the FTC truly cannot address without new legislative authority. In particular, the FTC ought to explain the scope of harm under the unfairness doctrine.

3. Require the FTC to do more to explain its application of the unfairness and deception doctrines in the future, such as through regular updates to these guidelines, better justifying consent decrees, and issuing no-action letters and advisory opinions.
4. Craft new legislation, if at all, to address (1) non-conjectural harms that cannot be addressed by a more robust development of quasi-common law by the FTC, (2) that are not outweighed by countervailing benefits, and (3) that consumers themselves cannot reasonably avoid—in other words, to focus a realistic assessment of costs and benefits, and a preference for user empowerment over regulation. This is the basic concept behind the unfairness doctrine but there may well be harms that do not fit into the unfairness doctrine that nonetheless merit government intervention—and that would be better addressed through targeted legislation than by attempting to shoehorn them into unfairness by expanding the definition of "substantial injury." For example, this might include restrictions on employers' ability to obtain the social networking credentials of their employees.
5. Explore the use of "smart disclosure" to empower consumers through greater transparency as an alternative to prescriptive mandates, starting with increasing the kinds of information collected by data brokers (properly defined).
6. Ensure that self-regulation in name does not become *co*-regulation in fact, where government regulates by having final approval to certify industry codes of conduct—or simply through extra-legal pressure. No matter how well-intentioned, "agency threats" undermine the rule of law.

In addition, Congress should take two other steps:

7. Support education - If the problem is a lack of consumer awareness, Congress should fund consumer education campaigns, as it has done in the past for privacy and child safety.
8. Focus on getting government's house in order - the greatest threat to our privacy lies with government itself, in that Congress has failed to update laws intended to extend Fourth Amendment Protections to data held by third parties.[5]

---

[4] Dept. of Justice, Guidelines and Policy Statements, http://www.justice.gov/atr/public/guidelines/.

[5] See Joint Letter to S. Comm. on Judiciary in support of ECPA Reform (Sep. 17, 2012), at http://net.educause.edu/ir/library/pdf/EPO1212.pdf.

Elaboration upon these points follows immediately below.

FTC Resources & Expertise

Congress should assess whether the FTC has adequate institutional resources and expertise. If the FTC had heeded Peter Swire's call for the FTC to build a an office of information technology five years ago,[6] our layered privacy approach would today be far more effective in protecting consumers and ensuring their trust, and less easily dismissed as inadequate by foreign privacy regulators. Chairman Leibowitz deserves credit for appointing the agency's first Chief Technologist. But even with someone as talented as Ed Felten in that position, the FTC is still way behind the curve: His title was not Chief Technology *Officer* because there is no office behind him to support the agency.

The FTC needs a clear strategic plan outlining:

1. How to build the in-house technical expertise it needs (beyond basic IT infrastructure) to identify enforcement actions, support successful litigation, monitor compliance, and conduct long-term planning and policy work, and

2. The resources necessary to achieve that goal through a combination of re-prioritizing current agency spending and additional appropriations.

Importantly, this organization should function as a cohesive team that meets the needs for technical expertise of all the FTC's bureaus and offices (including the Bureau of Competition). A stand-alone organization could, like the Bureau of Economics, better attract and retain talent.

FTC Quasi-Common Law

The proper measure of the FTC's effectiveness is not how many suits it successfully settles, but how well it builds a quasi-common law of privacy that can guide companies pushing the envelope with new data-driven technologies—without stifling innovation that ultimately serves consumers. The chief problem today is that we have essentially no privacy case law to look to, so companies have only FTC complaints and consent decrees to guide them in predicting the course of privacy law. These documents offer very little explanation of how the facts of a particular case satisfy the FTC's Policy Statements on unfairness and deception. And these summary assertions are never tested in court (at least until the recent *Wyndham* case), both because of the cost of litigation relative to settlement, and because of the cost to a defendant company of bad publicity from being perceived as anti-privacy exceed the benefits of taking the FTC to court—even when they would likely prevail given the FTC's overreach. While this should

---

[6] Peter Swire, *Funding the FTC: Globalization and New Information Technologies Necessitate an Appropriations Boost*, Feb. 26, 2007, http://www.americanprogress.org/issues/2007/02/ftc.html.

reassure us that reputation markets exert far greater pressure to discipline companies on privacy than is commonly appreciated,[7] it also means that we lack the key ingredient for building a true common law: judicial scrutiny in an adversarial process.

It is possible that Wyndham's pending challenge may clarify some of these issues.[8] But unless the court significantly curtails the scope of the FTC's authority, which seems unlikely given the facts of the case, this case may well be only a brief interruption to the general and long-established pattern of the FTC acting without judicial scrutiny. The forces that keep privacy adjudication out of the courts and prevent development of privacy common law by judges are not likely to be easily overcome by FTC—or even Congressional—action. So we need to find alternative ways to replicate the adversarial process of careful analysis by which courts build upon simple rules to address the challenges of a complex world. I suggest the following nine possible ways for the FTC to make better use of its existing authority to build a quasi-common law:

1. The Commission (or individual Commissioners) should provide greater analysis of its rationale under its Unfairness and Deception Policy Statements for issuing each consent decree.

2. Congress should hold hearings to explore how the model of the Tunney Act could be applied to consumer protection settlements, to require judicial approval of the consent decrees by which the FTC builds the quasi-common law of privacy, just as the DOJ must get approval for antitrust settlements.[9] This would ensure some degree of oversight of the Commission's legal analysis—and give the agency an incentive to explain that analysis more.

3. The FTC should, when it closes an investigation by deciding not to bring a complaint, issue a "no action" letter explaining why it decided the practice at issue was lawful under Section 5.[10] Such letters, issued by other agencies like the Securities and Exchange Commission, provide an invaluable source of guidance to innovators. Congress should even consider requiring the FTC to issue such letters.

4. The FTC should consider how it could use advisory opinions more effectively to provide guidance to industry on how the agency might evaluate new privacy practices—especially for companies working on the cutting edge of technology, which are often

---

7 See Daniel Klein, *Reputation: Studies in the Voluntary Elicitation of Good Conduct* (1997), at http://books.google.com/books/about/Reputation.html?id=p3gUN-oD2n0C.

8 *See* FTC v. Wyndham, Case No. CV 12-1365-PHX PGR (D. Ariz.).

9 15 U.S.C. §16 (2012).

10 See, e.g., Jodie Bernstein, Re: Petition Requesting Investigation of, and Enforcement Action Against SpectraCom, Inc., http://www.ftc.gov/os/1997/07/cenmed.htm.

small and early-stage. The FTC issues such letters on a wide range of topics,[11] yet does not appear to have issued advisory opinions regarding the application of Section 5 to privacy.

5. Congress should reassert the vital oversight it exercised in 1980 and 1983 when it ordered the agency to issue the Policy Statements on Unfairness and Deception. At a minimum, the FTC should be required to explain, in detailed analysis, how it has applied those venerable standards in past privacy enforcement cases, and how it plans to do so in the future—because it is "easier to learn from history than it is to learn from the future."[12] Such guidelines are routine in other areas, and provided for in the Commission's current procedures.[13] Indeed, the antitrust guidelines issued by the FTC and DOJ form a key element of the American common law of competition. The FTC has issued a number of Guides[14] to explain its approach to consumer protection—but none for consumer privacy.[15] The FTC's recently issued Privacy Report is no substitute for such a Guide because it describes what companies ought to do on privacy rather than how the FTC has decided companies must not act, and why. Indeed, the Report has little grounding in the twin Policy Statements that are supposed to be the FTC's lodestars. To replicate some of the adversarial nature of actual litigation, the process of drafting such guidelines must be the result of a substantive dialogue with affected stakeholders, and it must be subject to involved oversight from the full Commission and from Congress.

6. In particular, the FTC must clarify the boundaries of privacy harm under the Unfairness Doctrine. The FTC's leadership seems to be trying to have it both ways: playing down publicly what the agency can do with its existing legal authority (to support their argument for new statutory authority) while, at the same time, making bold claims about the scope of harm in their enforcement actions. If the concept of harm is

---

[11] 16 C.F.R .§ 1.1 (2012) ("Any person, partnership, or corporation may request advice from the Commission with respect to a course of action which the requesting party proposes to pursue. The Commission will consider such requests for advice and inform the requesting party of the Commission's views, where practicable, under the following circumstances... (1) The matter involves a substantial or novel question of fact or law and there is no clear Commission or court precedent; or (2) The subject matter of the request and consequent publication of Commission advice is of significant public interest."); see also Judith A. Moreland, Overview of the Advisory Opinion Process at the Federal Trade Commission, available at http://www.ftc.gov/bc/speech2.shtm.

[12] Quoted in Virginia Postrel, The Future and Its Enemies: The Growing Conflict Over Creativity, Enterprise, and Progress at 48 (Touchstone 1998).

[13] Federal Trade Comm'n, FTC Operating Manual §8, *available at* http://www.ftc.gov/foia/ch08industryguidance.pdf.

[14] Federal Trade Comm'n, FTC Bureau of Consumer Protection - Resources: Guidance Documents, http://ftc.gov/bcp/menus/resources/guidance.shtm (last visited June 26, 2012).

[15] Federal Trade Comm'n, Legal Resources | BCP Business Center, http://business.ftc.gov/legal-resources/48/33 (last visited June 26, 2012).

stretched too far, the Unfairness Doctrine will become again, as it was in the 1970s, a blank check for the FTC to become a "second national legislature" capable of regulating business practices across the economy.[16] I explained my concerns about the potential for the unfairness doctrine to be abused, but also my belief that the doctrine should be used to the greatest extent with the 1980 Policy Statement, in my March testimony before this Committee.[17]

7. Hold a public workshop on how the FTC could use its existing Magnuson-Moss rulemaking powers[18] to apply the Unfairness and Deception Doctrines industry-wide, rather than through adjudication.

8. Congress should hold hearings to explore making the FTC subject to the same cost-benefit analysis that all Executive Branch agencies have long been required to perform (but not independent agencies like the FTC and FCC).[19] Ideally, such a requirement should apply in some form to all consent decrees, since these are the key means by which the FTC regulates, but at a minimum, the requirement should apply to all reports issued by the FTC.

9. Congress should ensure the FTC has the adequate resources to engage in this detailed analysis. To dismiss the current legal model as inadequate simply because it has not been fully utilized, and to adopt instead a new legislative framework whose true costs are unknown, would be truly "penny wise, pound foolish." Given the clear need to reduce federal spending across the board, and the decidedly mixed record of antitrust law in actually serving consumers, Congress could simply reallocate funding from the FTC's Bureau of Competition—or, more dramatically, consolidate antitrust enforcement at the DOJ and allocate the cost savings from streamlining to the FTC's Bureau of Consumer Protection.[20]

I expand upon some of these suggestions below.

---

[16] *See generally* Howard Beales, III, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, § III, http://www.ftc.gov/speeches/beales/unfair0603.shtm [hereinafter Beales Paper]).

[17] *See* Szoka Testimony I, *supra* note 1.

[18] See generally, *FTC Operating Manual*, Chapter 7, http://www.ftc.gov/foia/ch07rulemaking.pdf

[19] Executive Order 13563 -- Improving Regulation and Regulatory Review, *available at* http://www.whitehouse.gov/the-press-office/2011/01/18/improving-regulation-and-regulatory-review-executive-order.

[20] *See* William E. Kovacic, *The Institutions of Antitrust Law: How Structure Shapes Substance*, 110 Mich. L. Rev. 1019, 1034 (2012) (identifying several problems with federal duality of antitrust jurisdiction).

Codification When Necessary

As explained by Nobel Prize winner, F.A. Hayek, in *Law, Legislation, and Liberty* (1973), the common law is the best system for coordinating the behavior of persons in light of dispersed knowledge. Legislation is best used to correct established problems resulting from the common law.[21] The FTC should first allow a quasi-common law of privacy to emerge before pushing for legislation to correct a problem which may not exist. While many would insist that the FTC model has failed, necessitating legislation, I do not think we can say the FTC model has really been tried until the FTC is required—either by Congress, by the courts, or perhaps by a Chairman with a very different approach—to explain its analysis thoroughly and consistently. Codification of common law can be useful to promote certainty in the law, but first the common law must be allowed to develop.

Rather than dismissing its existing Magnuson-Moss rulemaking authority[22] as "medieval" in order to justify Chairman Leibowitz's push for streamlined rulemaking authority,[23] the agency should make use of the powers it already has to help create this quasi-common law using its Section 5 authority to prosecute "Unfairness" and "Deception", as outlined above.

If the FTC uses this power to the fullest, it will reveal those areas where codification is appropriate—either by Congress or by the FTC itself. The latter means actually using Magnuson-Moss to issue rules when appropriate. The relevant section of the FTC Operating Manual merits inclusion here:

> WHEN IS PROMULGATION OF AN INDUSTRY-WIDE RULE APPROPRIATE?
>
> When staff becomes aware of allegedly unfair or deceptive acts or practices that appear widespread, it should consider whether rulemaking, as contrasted with adjudication, is appropriate. Some of the relevant factors to be considered include:

---

[21] Hayek argued that in certain cases the developed common law "may prove too slow to bring about the desirable rapid adaptation of the law to wholly new circumstances," and may lead into intellectual dead ends that are "seen to have undesirable consequences or to be downright wrong"—and in such cases it may be improved upon by legislation. *See* 1 FRIEDRICH A. HAYEK, LAW, LEGISLATION AND LIBERTY 88 (1973).

[22] See generally, *FTC Operating Manual*, Chapter 7, http://www.ftc.gov/foia/ch07rulemaking.pdf

[23] Beth DeSimone, *FTC Chairman Calls for Expanded Consumer Protection Powers over the Financial Services Industry*, Consumer Advertising Law Blog, February 10, 2010, http://www.consumeradvertisinglawblog.com/2010/02/ftc-chairman-calls-for-expanded-consumerprotection-powers-over-the-financial-services-industry.html.

> (1) Prevalence of the acts or practices under investigation. When a practice exists on a widespread basis, rulemaking has advantages over case-by-case adjudication... The precise degree of prevalence appropriate for undertaking a [rulemaking] will vary according to such factors as seriousness of consumer injury, vulnerability of the affected consumer group, amount of money involved in the given transaction, and severity of the contemplated rule's impact both on the affected industry, in general and especially on those industry members who did not engage in the underlying unfair or deceptive practices.
>
> (2) Cost of industry-wide investigation and rulemaking proceedings.
>
> (3) Feasibility of enforcement of the [industry-wide rule] by the Commission

Perhaps most important for the FTC to consider is the degree of "prevalence" required relative to the other factors provided.

Some in industry will doubtless object to any use of Magnuson-Moss, for fear that the FTC will repeat the overreach of the 1970s (when the agency ran wild with its unfairness jurisdiction).[24] Some consumer advocates may object that these procedures work too slowly, and, like some inside the Commission itself, worry that a revival of Magnuson-Moss could undermine efforts to pass new legislation, either comprehensive consumer privacy legislation or expansions of the FTC's powers. But neither should fear the FTC's use of Magnuson-Moss: So long as its essential procedural safeguards are kept in place, it is a difficult statute for the FTC to abuse. On the other hand, privacy advocates might have been able to achieve some of their legitimate demands for greater consumer protection already if they had started that process several years ago, instead of simply pushing for legislation in every new Congress.

If, for example, it can be shown that industry self-regulation permits practices that should be prohibited under the Unfairness Doctrine, the Commission should begin a Magnuson-Moss proceeding to ban them. Even the threat of doing so would likely be enough to cause self-regulatory bodies to update their codes of conduct. Thus, as always, self-regulation could work more expeditiously than government regulation—but the threat of regulation could spur self-regulation on.

Agency Threats

If the Commission could actually stake out a strong case, this would be a legitimate use of an "agency threat" because the pressure brought to bear would be (a) the use of process

[24] *See generally* Howard Beales, III, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, § III, http://www.ftc.gov/speeches/beales/unfair0603.shtm [hereinafter Beales Paper]).

established by law (Magnuson-Moss rulemaking) (b) justified under well-established legal doctrine. If the Commission's case was not strong enough to survive a legal challenge, the threat would probably not be credible enough to force changes to self-regulation.

But this is a far narrower conception of agency threats than that recently offered by law professor Tim Wu, who famously coined the term "net neutrality" and more recently served as a special advisor at the FTC.[25] As a descriptive matter, Wu is quite right that agencies do use such threats; but whether they should is a question that would make a fine subject for a hearing.

This Commission has made ample use of its soft power to influence Internet governance. In particular, the Commission has played a significant role in shaping the proceedings of the Worldwide Web Consortium's Tracking Protection Group. In September, nine Members of Congress sent a letter to FTC Chairman Jon Leibowitz asking seven questions about the FTC's role in the TPWG.[26] Leibowitz quickly responded with a letter answering several of the questions and promising to follow up with answers to the most difficult questions—about the FTC's communications and meetings with industry players or the W3C about DNT outside of W3C meetings.[27] The FTC has not yet followed up, nearly a month later, leaving unresolved the critical question of what role the FTC played in Microsoft's surprising decision to violate the consensus underpinning the W3C Do Not Track Process by turning on DNT:1 by default in its Internet Explorer 10 browser. In short, Congress has attempted to exert oversight over the agency's extra-legal activities, but apparently without success. This is a disturbing precedent because the FTC seems to be helping certain incumbents gain competitive advantage through a self-regulatory process.

Smart Disclosure

The clearer privacy promises are, the more easily the FTC will be able to enforce them. One important way to achieve this goal would be for the FTC to promote the use of "smart disclosure"—the term used by Cass Sunstein, director of the Office of Information and Regulatory Affairs, a close advisor to President Obama, and a widely respected thinker in law,

---

[25] *See* Tim Wu, *Agency Threats*, 60 Duke L. Rev. 1841 (2011), *available at* http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1506&context=dlj

[26] Letter of Rep. Tom Graves, Rep. Mick Mulvaney, Rep. Reid Ribble, Rep. Marsha Blackburn, Rep. Tim Walberg, Rep. Tim Huelskamp, Rep. Jeff Duncan, Rep. Dennis Ross, Rep. Dan Burton to Jon Leibowitz, Sept. 21, 2012, available at http://www.adotas.com/2012/09/members-of-congress-question-whether-ftc-is-attempting-a-dnt-end-around/

[27] Letter of Jon Leibowitz to Rep. Marsha Blackburn, Sept. 27, 2012, copy on file with author.

policy and technology. Smart disclosure can empower consumers by letting software do the work of reading privacy policies for them—and then implement their privacy preferences. Sunstein offers the following definition:

> the timely release of complex information and data in standardized, machine readable formats in ways that enable consumers to make informed decisions. Smart disclosure will typically take the form of providing individual consumers of goods and services with direct access to relevant information and data sets. Such information might involve, for example, the range of costs associated with various products and services, including costs that might not otherwise be transparent. … In many cases, smart disclosure enables third parties to analyze, repackage, and reuse information to build tools that help individual consumers to make more informed choices in the marketplace.[28]

While the creation of smart disclosure would probably be best done by self-regulation in light of the complexity of drafting disclosure formats, one area the FTC could be useful is in defining the structured data format for general disclosures or by mandating disclosure of privacy practices.

For example, users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app accedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct. As the FTC Privacy Report notes, smart disclosure could also "give consumers the ability to compare privacy practices among different companies."[29] An app store might illustrate how such comparisons could work, allowing users trying to choose between several competing apps to compare their privacy practices side by side.

While it would be preferable for smart disclosure to arise through self-regulation, especially given the complexity of crafting disclosure formats, mandating disclosure of privacy practices

---

[28] Cass R. Sunstein, Memorandum for the Heads of Executive Departments and Agencies 2 (Sept. 8, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/inforeg/for-agencies/informing-consumers-through-smart-disclosure.pdf.

[29] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 62 ("FTC Report"), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

would generally be a better way for government to address demonstrated market failures than by dictating what constitutes fair information practices. Thus, this might be an appropriate area for Congress to explore legislation if industry should fail to produce, and adopt, appropriate smart disclosure formats on their own.

2. You testified that the privacy debate has been biased by overstating the risks of harm and understating the benefits. How would you go about evaluating those factors? Is it possible to evaluate the benefits of future technologies?

This is, indeed, the key question on which tech policy analysts should focus. Among the benefits of data which have not been adequately considered in this debate are the following:

1. Enhanced advertising revenues for publishers of content and services that might otherwise have difficulty funding their offerings by charging for data, especially in markets where marginal costs are lower or zero (and basic economic theory would suggest that competition will inevitably drive prices towards zero).
2. More effective advertising, which in turn means:
    a. More relevant, and potentially less annoying/interruptive advertising for consumers;
    b. Better correlation between the production of content and services, and consumer preferences;
    c. Lower prices for consumers and greater innovation throughout the economy;
    d. More effective non-commercial messaging, including political speech accorded the highest protection by the First Amendment; and
    e. More vibrant media and improved political discourse and communities
3. Serendipitous innovation based on the discovery of unexpected uses of data.

But it is impossible to categorize all the benefits of technology, because they are largely unseen. The danger is that policymakers will focus on the seen risks of harm while understating unseen benefits, including future innovation. Frédéric Bastiat (1801-1850), the great French popularizer of economics, put it best when he wrote, in 1848:

> In the economic sphere an act, a habit, an institution, a law produces not only one effect, but a series of effects. Of these effects, the first alone is immediate; it appears simultaneously with its cause; it is seen. The other effects emerge only subsequently; they are not seen; we are fortunate if we foresee them. There is only one difference between a bad economist and a good one: the bad economist confines himself to the visible effect; the good economist takes into

> account both the effect that can be seen and those effects that must be foreseen.[30]

Developing the capacity to understand and effectively regulate technology is as much about ensuring that regulators understand how innovative technology confers benefits on consumers as it is about ensuring that regulators understand how new technology *doesn't* impose imaginary costs. As technological advance brings about ever more effective means of collecting and analyzing information, there is a tendency to view this through the lens of harm—to see such advances as ever more intrusive and potentially harmful. Forty years ago, the great economist Ronald Coase warned us:

> If an economist finds something—a business practice of one sort or another—that he does not understand, he looks for a monopoly explanation. And as in this field we are very ignorant, the number of understandable practices tends to be very large, and the reliance on a monopoly explanation, frequent.[31]

The same risk arises here—that, finding a technology that they don't understand, regulators will look for a nefarious (or "unfair") explanation, overestimating harms to users (the more easily seen) and understating benefits (the more likely unseen). Ensuring that regulators have the capacity to keep up with technological change is thus essential to facilitating both effective and appropriately restrained enforcement. This is what separates good policymakers from bad policymakers.

Of course it is impossible to fully anticipate the benefits of new technologies—because it is impossible to conceive of what new technologies might be developed, and how they might change the basic paradigms shaping the role of technology in our lives. The most important thing is for policymakers to adopt a posture of humility about technology. TechFreedom recently joined a number of other civil society groups from around the world in a Declaration of Internet Freedom, which began with the following two core principles:

> **Humility**. First, do no harm. No one can anticipate what the future holds and what tradeoffs will accompany it. Don't meddle in what you don't understand — and what you can all too easily break, without even seeing what's been lost. Often, government's

---

[30] Frederic Bastiat, *What is Seen and What is Not Seen* (1848), http://www.econlib.org/library/Bastiat/basEss1.html

[31] Ronald Coase, *Industrial Organization: A Proposal for Research*, *in* 3 POLICY ISSUES AND RESEARCH OPPORTUNITIES IN INDUSTRIAL ORGANIZATION 59, 67 (Victor Fuchs ed. 1972).

> best response is to do nothing. Competition, disruptive technological change, and criticism from civil society tend to resolve problems better, and faster, than government can.
>
> **Rule of Law**. When you must intervene, start small. Regulation and legislation are broad, inflexible, and prone to capture by incumbent firms and entrenched interests. The best kind of "law" evolves one case at a time, based on simple, economic principles of consumer welfare — alongside the codes of conduct and practices developed by companies under pressure from competitors and criticism. Worst of all, when regulators act without legal authority, or regulate by intimidation, they undermine the rule of law, no matter how noble their intentions.

Commissioner Ohlhausen expressed admirable humility in her first testimony after being confirmed to the Commission:

> Clearly, the technology sector is developing at lightning speed and we now face issues unheard of even a few years ago. I wish to proceed cautiously in exploring the need for any additional general privacy legislation, however. I have concerns about the ability of legislative or regulatory efforts to keep up with the innovations and advances of the Internet without also imposing unintended chilling effects on many of the enormous benefits consumers have gained from these advances or without unduly curtailing the development and success of the Internet economy.[32]

The best way for regulators to protect consumers in a constantly evolving world, without chilling technological change, is to follow the common law method of case-by-case adjudication based on the very doctrines the FTC already has in place: deception and unfairness. But this is why, as explained above, it is so critical that the FTC do more to explain its conception of "substantial injury" as well as "countervailing benefit"—and how to balance the two. This is no easy task and it is not something that can be written down once and for all. But over time and with the proper scrutiny (ideally from the courts), the FTC could develop a framework to do just this.

---

[32] *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (2012) (statement of Maureen K. Ohlhausen, Commissioner, Federal Trade Commission), at 4, *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=0b54f847-1e2f-4bee-8d3f-21581465c1f1.

3. There are some types of harm we protect against before it happens. For instance, we lock our car doors but what are the odds of a carjacking? We lock the doors to our homes at night, but how many of us have had our homes invaded? Why should the Federal government not establish baseline rules to guard against the harm of someone accessing damaging or potentially embarrassing information about private citizens as gleaned from search history, online shopping habits, or e-book purchase or video viewing history?

Congress has already addressed certain categories of harm through targeted legislation, such as the Fair Credit Reporting Act and the Video Privacy Protection Act. Even if the basic rationale behind both laws was sound, neither has aged particularly well.[33]

The VPPA, in particular, offers an object lesson in the dangers of legislating specific prescriptions in advance of a technology's development rather than allowing regulators to intervene on a case-by-case basis according to basic principles like unfairness and deception. Passed as a prophylactic response to an incident involving the failed Supreme Court nominee Robert Bork,[34] the VPPA has prevented Netflix from empowering U.S. users to share with their friends what movies they're watching, just as users of Spotify and other services can do with music and other content they're enjoying. Yes, this particular problem appears likely to be remedied soon, with the passage of Sen. Leahy's Video Privacy Protection Amendments Act.[35] But how many other problems go unnoticed, or unaddressed because companies less influential than Netflix cannot make an issue like this even rise above the noise level in Washington? How many startups are never founded because outdated legal requirements like this prevent them from receiving funding? These are all unseen costs of laws that attempt to prevent against speculative future harms.

Congress has already "establish[ed] baseline rules to guard against" real harms—that is the essence of Section 5. But to date, the FTC has done a poor job of conceptualizing harm, as discussed above. The Commission could do much more to explain what it means by harm, and thus protect against harms before they happen without falling into the trap of trying to specifically prescribe speculative harms.

---

[33] *See* Jim Harper, *Reputation Under Regulation: The Fair Credit Reporting Act at 40 and Lessons for the Internet Privacy Debate*, Cato Policy Analysis No. 690 (Dec. 8, 2011), *available at* http://www.cato.org/pubs/pas/PA690.pdf.

[34] *Video Privacy Protection Act: Introduction*, Electronic Privacy Information Center, http://epic.org/privacy/vppa/ (the VPPA "was passed in reaction to the disclosure of Supreme Court nominee Robert Bork's video rental records in a newspaper.").

[35] S. 3414, 112th Cong. (2012), *available at* https://www.cdt.org/files/pdfs/Leahy-ECPA-Amendment-S3414.pdf.

But again, legislation should be a last resort after it can be shown that a quasi-common law of privacy is insufficient to deal with the problem. First, the FTC should focus on defining harm clearly in order to establish baseline rules to protect privacy. The FTC should help to clarify this uncertainty by convening a public workshop on its unfairness authority, with a special emphasis on defining the boundaries of cognizable harm. Ideally, such a workshop would produce guidelines building on the 1980 Unfairness Policy Statement adequate to help companies predict how to build new and innovative services without running afoul of the unfairness authority. In essence, the workshop should address the questions raised by Commissioner Ohlhausen in her first testimony after being appointed to the Commission:

> "What harms are occurring now that Section 5 cannot reach and how should harm be measured? As my colleague Commissioner Rosch noted in his dissent to the Privacy Report, the Commission has specifically advised Congress that absent deception, it will not enforce Section 5 against alleged intangible harm, (FTC letter to Ford and Danforth, 1984), and the FTC's own unfairness statement suggests that the focus should be on monetary as well as health and safety harms, rather than on more subjective types of harm. Although the Commission's Privacy Report did not reject the fundamental insights of the harm-based approach, it appears to embrace an expansion of the definition of harm to include 'reputational harm,' or 'the fear of being monitored,' or 'other intangible privacy interests' (*see* Report at iii, 20, 31), and, as an initial matter, I have reservations about such an expansion."[36]

The basic analytical framework of the Unfairness Doctrine itself should guide Congress in determining how to supplement the Unfairness Doctrine with legislation targeted at harms that cannot properly be addressed through the Unfairness Doctrine directly—i.e., without stretching the definition of "substantial injury." In other words, just because a harm does not neatly fit within the unfairness doctrine (say, employer access to employees' social media passwords), does not mean it may not be a valid target for legislation; but even in such cases, lawmakers should still weigh that harm against countervailing benefits and intervene only where consumers themselves cannot reasonably avoid the harm, such as through increased transparency and more effective privacy controls.

4. The FTC applauds industry efforts to develop a Do-Not-Track mechanism, however, the Chairman recognized that the industry-developed mechanism is merely an opt-out of

[36] Ohlhausen, *supra* note 30, at 3.

behavioral targeted ads and suggests that such mechanisms should enable consumers to opt out of information collection as well. Most consumers who are bothered by behavioral targeted ads are not troubled by the ad itself but rather by how the ad network knew that particular ad would interest the consumer. If we accept that as true, how is the industry-developed Do-Not-Track mechanism responsive to consumers' privacy concerns when it only stops the delivery of ads but not the collection of the underlying interest information?

It is true that "Do Not Track" is something of a misnomer: the technical specification under development by the Worldwide Web Consortium (W3C) is actually a use-specification mechanism. A true "Do Not Track" mechanism would essentially be an ad-blocker, since blocking *all* tracking makes even the simplest forms of online advertising impossible, because even "contextual" advertising requires tracking of views. Thus, a tool that blocked tracking elements but not the display of ads themselves would still break online advertising. In fact, such mechanisms are already readily available to consumers, most notably the browser plug-in AdBlock Plus, which has nearly fifteen million users on Firefox,[37] and over five and a half million users on Chrome.[38] These users are essentially free-riding on users who don't block ads. Adblocking is, simply put, a form of piracy. As Ken Fisher, the founder & Editor-in-Chief of Ars Technica, eloquently put it:

> Imagine running a restaurant where 40% of the people who came and ate didn't pay. In a way, that's what ad blocking is doing to us. Just like a restaurant, we have to pay to staff, we have to pay for resources, and we have to pay when people consume those resources. The difference, of course, is that our visitors don't pay us directly but indirectly by viewing advertising.[39]

There is simply no reason government should promote the use of such adblocking tools. Fortunately, such mechanisms are still used by only a relatively small percentage of the overall population—below the acceptable loss threshold for most publishers (the point at which it becomes cost-effective for publisher to try to make explicit today's implicit quid-pro-quo). It is far from clear what will happen above that threshold, whether an architecture of explicit negotiation between sites and users (such as contemplated by the "user-granted exception" features of the Do Not Track spec currently being drafted) will produce the same quantity and

---

[37] Ad Block Plus Add-on for Mozilla Firefox, https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/.

[38] Adblock Plus (Beta), https://chrome.google.com/webstore/detail/adblock-plus-beta/cfhdojbkjhnklbpkdaibdccddilifddb.

[39] Ken Fisher, *Why Ad Blocking is devastating to the sites you love*, arstechnica (Mar. 6, 2010), http://arstechnica.com/business/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love/.

distribution of revenue. In other words, far from simply facilitating users' preferences, such a system may produce outcomes that users would not have chosen on their own—primarily because the increased transactions costs involved may swamp the relatively small value created by each interaction between site and user. Thus, forcing such a change may fundamentally change the nature of the Internet ecosystem.[40]

The essential disconnect here between "consumers' privacy concerns" and technical reality is that the information collected is the same in both cases; it is simply a question of the use to which it is put. The question, then, is what sorts of uses (including data retention and sharing) consumers are opting out of when they send a DNT:1 header saying "Don't track me."

What the Digital Advertising Alliance committed to do in February was to honor signals sent by a DNT:1 header as an opt-out from the use of information about a user's browsing behavior to display behavioral advertising.[41] The W3C's Tracking Protection Working Group (in which I participate as an invited expert) is currently working on developing a technical specification as to exactly what DNT:1 will mean. While the TPWG has to define the term "tracking," it is clear that it will be essentially consistent with the DAA's definition: "Online Behavioral Advertising does not include the activities of First Parties, Ad Delivery or Ad Reporting, or contextual advertising (i.e. advertising based on the content of the Web page being visited, a consumer's current visit to a Web page, or a search query)."[42]

It is worth noting that the DAA has two self-regulatory codes of conduct: the other, Self-Regulatory Principles for Multi-Site Data, issued in November 2011, protects all consumers, whether or not they exercise an opt-out, by specifically restricting the use of data collected across websites for eligibility for employment, credit, health care, or insurance, and requires consent for children's information (consistent with COPPA) as well as health and financial data.

---

[40] *See* Appendix below; Berin Szoka, *The Paradox of Privacy Empowerment: The Unintended Consequences of "Do-Not-Track"* (Position paper for W3C Workshop: Do Not Track and Beyond, Berkeley, California, November 26-27, 2012).

[41] Press Release, Digital Advertising Alliance, White House, DOC and FTC Commend DAA's Self-Regulatory to Protect Consumer Online Privacy: DAA Announces Plans to Expand Program Consumer Choice Mechanisms (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

[42] Interactive Advertising Bureau, et. al, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 11 (July 2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

The Honorable Cliff Stearns

1. Mr. Szoka, you testified that companies should be encouraged to educate consumers through more accessible forms of notice that explain privacy policies and practices. How can we as Congress encourage companies to do this?

As explained above, smart disclosure could bypass much of the current debate about the failure of effective notice to empower consumers by making "notice" technologically actionable: Users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, [43] which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app accedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct.

Congress should commission the FTC to issue a report on the feasibility of using structured data formats to facilitate actionable privacy disclosures. Such a report should be subject to public input through a workshop, and to review in draft form prior to being finalized. Ideally, the report would be developed by an Chief Technology Officer such as proposed above, with a technical expert in smart disclosure hired to lead work on this report. The report should assess lessons learned from the experience with P3P and the ongoing W3C Tracking Protection Working Group.

Of course, if Congress really wants to help to educate consumers, it can also support campaigns aimed at building consumer awareness. The FTC has conducted such campaigns in the past, such as its "Net Cetera: Chatting with Kids about Being Online" toolkit.[44] Congress could either appropriate money for further such campaigns or, more preferably, support a competitive grant-making program for civil society groups to run their own educational campaigns.

2. At the hearing we heard that allowing all consumers to access whatever data companies have about them presents significant technical challenges and could actually increase risk to consumers. But what about a narrower bill that would allow consumers to

---

[43] *See, e.g.*, Terms of Service - Didn't Read, http://www.indiegogo.com/terms-of-service-didnt-read (offering evaluations of online terms of service from a privacy perspective).

[44] Net Cetera Toolkit, OnGuardOnline, http://www.onguardonline.gov/features/feature-0004-featured-net-cetera-toolkit.

ask companies for categories of information that companies have on them. Wouldn't this alleviate the risk of harm to the consumer and burden on the company while at the same time help educate consumers on data collection?

The flipside of user access is privacy breach—and all that separates the two is effective authentication that the person attempting to access a record is the right person. Congress (and the FTC) should avoid creating new privacy problems in the name of privacy by mandating access or correction rights (two of the Fair Information Practice Principles) in situations where the user is not already authenticated, because doing so would, ironically, require *more* collection of personal information, and create new privacy problems.

Reducing the granularity of information subject to an access right certainly does reduce the potential privacy problem but it does not eliminate it. For example, Microsoft's Personal Data Dashboard (https://choice.live.com/data/) and Google's Ad Preferences Manager (www.google.com/ads/preferences/) both show users the interests associated with their profile (e.g., pets, travel, technology), but still require users to log-in to see even this relatively innocuous information.

As noted by the question, allowing consumers access to whatever data companies have on them could actually increase risk to consumers. If companies had to keep such individualized files tied to authenticated accounts, this could create a honeypot for potential identity thieves. Requiring a log-in, as Microsoft and Google do, would reduce the problem, but if identity thieves could gain access, they would have considerably more information available to them in one convenient location. Such honeypots could also attract the interests of law enforcement, which would probably be able to access them without a warrant because courts have ruled (wrongly) that the Fourth Amendment does not apply to "third party records,"[45] and the Electronic Communications Privacy Act has failed to keep pace as a substitute for Fourth Amendment protection.

So before crafting any kind of disclosure mandate, Congress would have to decide:

1. What kind of information merits a disclosure mandate. Any legislation should be very specific about the justification for mandating disclosure.
2. Whether the costs of disclosure outweigh the benefits.

[45] Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 Am. U. L. Rev. 1381 (2008), *available at* http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1045&context=aulr.

There certainly are circumstances when access—and even correction—rights are warranted, such as for credit records. A compelling case can be made for mandating such access by law, where the potential harms of inaccurate information are clear—e.g., eligibility for credit, the basis for the Fair Credit Reporting Act's access and correction mandate. But even then, Congress should be careful not to mandate these rights in such a way that would lead to ossification. As noted by Jim Harper, in his discussion of FCRA:

> Though the information and technology environments have changed dramatically over the last four decades, the credit reporting and reputation marketplace has seen little change or innovation. A potential related market for identity services is also stagnant thanks in part to government policies.[46]

It is difficult to equate the situation of online advertising with credit records, though—especially when the online advertising industry has barred data collected for advertising purposes from being used for employment, credit, health care treatment, or insurance eligibility decisions.[47] Inaccurate advertising and marketing data would at worst result in less relevant advertising. As a result, the costs associated with building the necessary infrastructure to permit access and correction rights for advertising and marketing data might significantly outweigh the benefits.

The legislation posited by the question seems to refer to the FTC Report's proposal regarding "data brokers":

> the data broker industry explore the idea of creating a centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options. This website will improve transparency and give consumers control over the data practices of companies that maintain and share data about them for marketing purposes.[48]

---

[46] Harper, *supra* note 31, at 1.

[47] Digital Advertising Alliance, SELF-REGULATORY PRINCIPLES FOR MULTI-SITE DATA (Nov. 2011), http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[48] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("FTC Report"), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf, at 69.

This concept merits exploration as a way of remedying the lack of transparency regarding companies that currently lack a direct way of offering transparency to those whose data they collect—provided the term "data broker" is defined appropriately. This could be an excellent test case for encouraging smart disclosure through self-regulation—but only if it can be implemented in a way that actually improves transparency for consumers and proves feasible for companies.

The term "data broker" was defined quite expansively in the FTC Privacy Report. As Linda Wooley, the executive VP of the Digital Marketing Association's Washington operations, rightly asked, "Data is changing the world, but I'm not sure the FTC can define what a 'data broker' is. Is a data broker Acxiom, Google or Macy's? All companies are sharing data in 2012. First parties are now doing collecting and having third parties crunch the data for them. Where do you draw the line?"[49] Drawing the line in the wrong place could lead to fundamental changes in the market for information—to the detriment of consumers.

It would be a mistake to focus on having a single website as an interface for transparency to consumers. Such a site could be built and advertised as a one-stop shop for consumers to learn more about what kinds of information data brokers collect. But it should be only one of many potential interfaces that can display, in a user-friendly way, information provided by data brokers in structured formats. In technical terms, such a site would merely be an aggregator of feeds of raw data provided by each data broker about their practices. For example, if data brokers provided descriptions of their data collection practices in standardized form at a standardized url, e.g., databroker.com/DCP.xml (for "data collection practices"—a parallel to the convention of website.com/RSS.xml), *any* privacy site or tool could pull those feeds automatically and present the information to users in helpful ways. This would be smart disclosure at its best.

3. Are you familiar with my bill, H.R. 1528, the Consumer Privacy Protection Act of 2011? This bill calls for clear, easy to understand privacy policy statements and provides for the FTC to approve a five-year self-regulatory program. Would you support this bill advancing through the Subcommittee?

---

[49] Christopher Hosford, *'Data Brokers' new target of FTC privacy recommendations*, BtoB (Apr. 2, 2012), http://www.btobonline.com/apps/pbcs.dll/article?AID=/20120402/DIRECT0101/303299993/data-brokers-new-target-of-ftc-privacy-recommendations&template=printart.

This bill does perhaps a better job than any of the other privacy bills introduced in this Congress at balancing the competing values at play. In particular, the bill wisely deems an IP address to be Personally Identifiable Information (PII) only when combined with one of the other true identifiers listed in the bill, such as name or email address. That said, I do have several concerns about the bill's likely effects—on both sides of the balancing act.

First, the bill it would convert the U.S. self-regulatory approach into something quite different: the European model of co-regulation. If the FTC must ultimately approve a self-regulatory standard, it will likely play the dominant role in drafting the standard. This will replace the "competitive discipline" of market and reputational pressures with agency threats as the driving factors behind setting codes of conduct. Like all such regulation, the bill risks creating regulatory ceilings above which companies have no incentive to compete with stronger privacy protections.

Indeed, the Digital Advertising Alliance has already implemented many of the practices the bill would require. So why is such intrusion warranted? Is the DAA not *less* likely to continue improving its self-regulatory system once it has been officially sanctioned by the FTC? Whatever the intentions of such an approval requirement, the lesson of regulated industries is clear: the more power an agency has to set approved standards of conducting business, the more prone it is to capture by entrenched interests to insulate themselves from further obligations as well as competition.

Second, the bill appears to take away the ability of consumers to enforce contractual privacy rights directly. Section 10 prescribes the terms of a dispute resolution process for entities in a self-regulatory program and Sections 11 and 12 exclude private rights of action with respect to alleged violations and preempt state laws. This puts a few members of the FTC bureaucracy in charge of privacy protection rather than the interactions of millions in the marketplace, subject to the evolving common law. As Jim Harper argued about FCRA:

> When the Fair Credit Reporting Act preempted state common law remedies against credit bureaus, it foreclosed an option that may have resulted in better protection for consumers and better results for the economy and society. Because Congress imposed a national credit reporting rule, we cannot know how this industry might have developed had it been left free to experiment, subject to simple rules against harming consumers.[50]

[50] Harper, *supra* note 31, at 2.

Third, one aspect of the bill may require clarification: Section 10 provides that "A violation of any provision of this Act by a covered entity is an unfair or deceptive act or practice unlawful under section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)), except that the amount of any civil penalty under such Act shall be doubled for a violation of this Act." Of course, Section 5(a)(1) does not provide for any monetary penalties (for acts or practices the FTC finds unfair or deceptive); only when a company has been placed under a consent order for such practices and violated that order may, under 5(a)(l), the Commission impose a monetary penalty (not more than $10,000 for each violation). Is H.R. 1528 intended to impose monetary penalties for (willful) violations of self-regulatory programs (i.e., double the penalty imposed by Section 5(a)(l) for violations of consent decrees)? If so, the language, or simply the cross reference to the FTC Act, should be clarified.

This is important because the threat of monetary penalties intersects with with the presumption of compliance created under the bill: the greater the risk of monetary penalties, the more a presumption of compliance makes sense; but too great a presumption of compliance is itself a problem, which may suggest reducing the presumption, and accordingly reducing the threat of monetary penalties.

Covered entities in self-regulation programs enjoy a strong presumption of compliance under the proposed bill (§ 9(a)(1)). This presumption may only be overcome by "clear and convincing evidence" of wilful non-compliance (§ 9(d)(4)). I agree that some presumption makes sense and have criticized the FTC for holding Google strictly liable (the opposite of a presumption of compliance) for statements it made about its privacy practices that became untrue only after Apple changed how Safari handled cookies.[51] But should a presumption really protect companies for, say, grossly reckless non-compliance with an industry standard? Might it not make sense for the presumption to give way, in part, if a self-regulatory body recommends that the FTC pursue an enforcement action—even if a company was not wilfully non-compliant? This shifting of traditional evidentiary standards will make it more difficult for the FTC and consumers to win close cases. Creating such a strong presumption may unduly create the impression that the bill exists merely to insulate industry from liability. This is another reason the contract law approach, supplemented with a quasi-common law of privacy from the FTC, would likely be more effective in promoting consumer welfare.

Fourth, the bill risks being tied up in litigation over its application to non-profit entities. Congress has heretofore largely avoided First Amendment challenges to its regulation of the

[51] Berin Szoka & Geoffre Manne, *FTC's Google Settlement a Pyrrhic Victory for Privacy and the Rule of Law*, TechFreedom (Aug. 9, 2012), http://techfreedom.org/node/195.

Internet by exempting non-profit entities from legislation. What is the rationale for including them here? This is especially problematic, given the Supreme Court's recent decision in *Sorrell*, ruling that privacy prior consent requirements for the use of interest data for prescription drug marketing violated the First Amendment. [52]

[52] Sorrell v. IMS Health, Inc., No. 10-779 (2011), http://www.supremecourt.gov/opinions/10pdf/10-779.pdf

TECH FREEDOM

The Paradox of Privacy Empowerment: The Unintended Consequences of "Do Not Track"

Position paper for W3C Workshop: Do Not Track and Beyond
Berkeley, California, November 26-27, 2012

Berin Szoka[53]

The debate over "Do Not Track" offers an excellent microcosm for understanding the larger privacy policy discourse. Arguments for giving users a tool to express their privacy preferences exert enormous rhetorical appeal. Those arguing for versions of DNT that are more restrictive of the collection and use of information about user behavior essentially insist that "We're merely giving users a choice!" Who could possibly be against letting users choose for themselves? Why should anyone else get to choose *for us*—especially companies that seem to be profiting from the ignorance or helplessness of users?

Tools like "Do Not Track" (and "privacy-friendly" interfaces more generally) are usually justified as simply offering users a means of expressing their true preferences. But such choice architectures[54] are anything but neutral: even with the best of intentions and in the name of facilitating user choice, choice architects will produce outcomes that users would not have chosen if they could make fully rational decisions in a frictionless world without transactions costs. This is the essential paradox of user empowerment.

"Privacy advocates" regularly cite opinion polls showing that users demand greater privacy protection—and thus conclude that privacy-friendly choice architectures simply facilitate the true preferences of users. But listening to what consumers *say* they want tells us much less about their preferences than seeing what preferences they *reveal* in the process of making real-world decisions about trade-offs among values. As much as users value privacy, they do not value privacy in isolation or inherently, but relative to other values—including other forms of privacy.

---

[53] This position paper draws testimony I gave to the Senate Commerce Committee in June 2012, http://techfreedom.org/node/185

[54] On term "choice architecture" and its inherent non-neutrality, *see generally* Richard H. Thaler University of Chicago, Cass R. Sunstein & John P. Balz, Choice Architecture, April 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1583509.

To avoid the paradox of user empowerment to the greatest extent possible, choice architects must understand how their proposed choice architecture will shape real-world outcomes, and the impact that will have on these many competing values. Let us consider the unintended consequences of three contested aspects of DNT:

1. **Default setting** - How, and by whom, may a browser be set to send DNT:1?
2. **Definition of tracking** - What is it DNT:1 tells servers not to do?
3. **Architecture of negotiation** - How do sites get users who send DNT:1 headers to opt-in to tracking—and to remain opted-in?

Each is a complicated issue. But all three may be understood, to a degree, in terms of the traditional opt-in and opt-out paradigms. DNT:1 is nothing more than a signal sent by the user's browser expressing a preference not to be "tracked," however defined—after which website publishers, advertisers and other data collectors must somehow negotiate with the user to get him or her to "opt back in" (a term actually used in the TPE[55]) to "tracking" (by granting a site or network a "user-granted exception"). If browsers and other user agents may turn on DNT:1 by default, then the adoption rate of DNT will quickly exceed publishers' "maximum acceptable loss threshold." Below that point it makes little practical sense for publishers and advertisers to bother building an architecture of negotiation, because it is more cost-effective to let DNT:1 users free-ride off those allow tracking (either by setting DNT:0 or by not having it set at all).

Put more simply, if browsers are allowed to turn DNT:1 on by default, most users will live in a world where "tracking" is opt-in. This will be a choice made *for*, not *by*, users. But either way, all of the problems of more general "Opt-In Dystopias" described by Nicklas Lundblad and Betsy Masiello would apply once DNT:1 is turned on. They distill their concerns into four categories:

> **Dual cost structure**: Opt-in is necessarily a partially informed decision because users lack experience with the service and value it provides until after opting-in. Potential costs of the opt-in decision loom larger than potential benefits, whereas potential benefits of the opt-out decision loom larger than potential costs.
>
> **Excessive scope**: Under an opt-in regime, the provider has an incentive to exaggerate the scope of what he asks for, while under the opt-out regime the provider has an incentive to allow for feature-by-feature opt-out.

[55] http://www.w3.org/TR/tracking-dnt/#exceptions-principles

> **Desensitisation**: If everyone requires opt-in to use services, users will be desensitised to the choice, resulting in automatic opt-in.
>
> **Balkanisation**: The increase in switching costs presented by opt-in decisions is likely to lead to proliferation of walled gardens.[56]

The problem is that DNT, like any choice architecture, affects not only "demand" (empowering users to choose) but also the "supply" (the choices available to users). The difficulty of obtaining opt-ins (user-granted exceptions) will serve as a barrier to entry, protecting larger, established incumbents against competition from new entrants. This will be true on some level for individual sites: absent dual-cost structure problem, one might think that any site a user visits will easily be able to get an opt-in. But obtaining such opt-ins is costly, both for user and for sites, which must implement a mechanism for obtaining user-granted exceptions. Some sites will simply decide not to risk alienating users, and forego potential additional revenue, while other better established sites or sites less subject to competition, will gain a competitive advantage.

But the greater problem lies with web-wide exceptions, opt-ins to data collection by an ad network or other data collector across the web. To be sure, these are essential to making DNT work without breaking business models that depend on third-party ad networks, but they will also necessarily favor certain established players in the data and advertising ecosystem over other, generally smaller players. One might dismiss these competitive effects as the necessary consequence of restructuring an industry that is loathed by many (despite the benefits it confers),[57] but this consolidation would likely be accompanied by a qualitative change in the *kind* of information collected. Once a network obtains a web-wide exception, why *not* collect more data across the web? Why not associate it in a richer profile? As Masiello and Lundblad explain:

> service providers may attempt to maximise data collection in every instance that they are forced to use an opt-in framework; once a user consents to data collection, why not collect as much as possible? And the increased transaction costs associated with opt-in will lead service providers to minimise the number of times they request opt-in consent.

---

[56] N Lundblad and B Masiello, "Opt-in Dystopias", (2010) 7:1 SCRIPTed 155, http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp

[57] See generally, Comments of Berin Szoka, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, Dec. 7. 2009 http://ftc.gov/os/comments/privacyroundtable/544506-00035.pdf

> In combination these two behaviours are likely to lead to an excessive scope for opt-in agreements. In turn, users will face more complex decisions as they decide whether or not to participate.[58]

Indeed, why not require users to log-in and provide more information about their real identity? Of course, requiring users to go through an account-creation process would likely turn off many users—if only because it took longer than simply clicking on a dialog box that asked about enabling personalized content. But consumers have become quite accustomed to using Single Sign On systems to log into websites with their Facebook, Twitter, Google or Microsoft Live accounts (and so on). It is not difficult to see such networks becoming federated content networks—the new walled gardens so feared by Tim Wu, Jonathan Zittrain and many others. Leaving a website inside one network and going to the other would require granting another web-wide exception to another network. This isn't necessarily bad but if it ultimately means that *more* information is collected about Internet users, DNT will leave many of its advocates sorely disappointed—and it is certainly not a result any user would have chosen.

This perverse potential (but likely) result simply one example of a larger problem: human rationality is bounded; we are simply not capable of weighing the full implications of choices as complicated as those over privacy. This does not mean that user empowerment is not a worthy goal; it is (and it is generally preferable to more top-down alternatives such as regulatory prescriptions on the use of data). But it *does* mean we should not pretend that choice architects are not, in fact, making important choices for users in the process of designing choice mechanisms like Do Not Track.

The problems described above will become more acute the more broadly "tracking" is defined, the more users turn on DNT:1, and the more cumbersome negotiation is. Two particular contested issues within the TPWG will significantly aggravate the opt-in dystopias problem:

1. **Default Settings** - Although the TPWG has always rested on the consensus that DNT headers must be set by users not user agents like browsers,[59] Microsoft breached that consensus earlier this year when it announced earlier this year that it would choose *for* users by setting DNT:1 on by default in its new IE10 browser. European regulators have

---

[58] *Opt-in Dystopias*.

[59] "The goal of this protocol is to allow a user to express their personal preference regarding tracking to each server and web application that they communicate with... Key to that notion of expression is that it MUST reflect the user's preference, not the choice of some vendor, institution, or network-imposed mechanism outside the user's control." TPE § 3.

essentially endorsed this position, calling for users to "told about any default setting; and prompted to keep or to change it"—even if that setting is DNT:1, and therefore not compliant with the DNT spec—and insisting that servers must not disregard DNT headers, even when sent by browsers that turn on DNT:1 by default.[60] It remains unclear how this issue will be resolved.

2. **Configuration** - The TPWG co-chairs recently rejected a proposal to clarify that, to "reflect the user's preference," user agents must "require equal effort to configure [DNT]"[61]—prompting the first formal objection filed in the TPWG.[62] Thus, unless this decision is ultimately reversed by the W3C, a user agent need not set DNT:1 by default if doing so proved problematic; it need only design a user interface that will achieve the same result.

Ultimately these concerns are likely to be dismissed by insistence that sites and services will simply negotiate around DNT to reach the same outcome they would have reached anyway. But in the real world (as opposed to a frictionless perfect market), transactions costs often swamp the gains created by transactions such as the negotiation between site and user. The online advertising ecosystem currently works because it generated tiny amounts of value from enormous volumes of transactions. Even the small transactions costs of forcing today's implicit quid pro quo to become explicit could produce dramatically different outcomes. Nor is it clear that negotiation or payments would generate as much revenue as advertising—meaning that rising transactions costs would be borne by publishers, and passed on to users in the form of reduced quality, quantity or innovation, or higher prices (if they can actually charge prices).

Building on Ronald Coase's seminal work on the importance of transactions costs, Harold Demsetz offered the basic insight that continues to guide the law and economics of setting defaults (which economists generally refer to as "property rights"): in a frictionless world, if the initial assignment of rights is inefficient, negotiation will inevitably and costlessly solve the problem; but in the real world, that initial assignment may prove sticky, thus we should not assign rights in ways that are inefficient.[63] Once again, choice mechanisms are not neutral. If, the day before Microsoft announced their decision to set DNT:1 by default, it was true that "majority default DNT is not the world this standard will exist in. DNT is going to be a 10%

---

[60] Neelie Kroes, An update on Do Not Track The Centre for European Policy Studies (CEPS)/Brussels, 11 October 2012, http://europa.eu/rapid/press-release_SPEECH-12-716_en.htm

[61] http://lists.w3.org/Archives/Public/public-tracking/2012Sep/0197.html

[62] http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0104.html

[63] Harold Demsetz, *Toward a Theory of Property Rights*, 57:2 Am. Econ. Rev 347 (1967).

[63] http://www.econ.ucsb.edu/~tedb/Courses/Ec100C/Readings/Demsetz_Property_Rights.pdf

solution,"[64] and DNT:1 creates the negative unintended consequences described above (among others), why should choice architects not set the initial assignment to the setting that is more likely to be efficient: DNT:1 *off* by default and not privileged when users configure their browser? An argument could be made to the contrary if it could be shown that "tracking" (as defined by the DNT spec) actually lead to real harm, but as yet, no such argument has been substantiated, and the question of harm has repeatedly been sidestepped within the TPWG.

It is understandable, if ironic, that privacy advocates should desire outcomes that could actually reduce privacy and make consumers worse off—because the chain of causation is attenuated and unclear compared to the noble intentions behind restrictive defaults. Nobody wins Nobel Prizes in Economics for explaining things that are completely obvious, and even once they do, it can take decades (or more) for their insights to permeate areas of discourse outside of economics—such as Internet standard-setting.

It is much more understandable what some market players have to gain by joining forces with well-intentioned but short-sighted privacy advocates: competitive advantage. This is simply another example of the well documented alliance of "bootleggers and baptists."[65] Microsoft, in particular, stands to lose little by disrupting the online advertising market, in which it has struggled to compete. It is by no means clear whether a world of high DNT adoption rates would benefit, in relative terms, Microsoft more than Google (or, for that matter, Facebook), but it might well help Microsoft, since it would generally favor large incumbents with directs relationships with users, such as through the browser and OS. And Microsoft would hardly be the first company to wager that it held a losing hand, and that its odds would be better with a fresh deck of cards.

What lies ahead for choice architects "beyond DNT?" The perpetually difficult task of weighing costs and benefits, and attempting to foresee the unpredictable, in shaping users' choices.

---

[64] *See* Lauren Gelman, "Re: tracking-ISSUE-150: DNT conflicts from multiple user agents [Tracking Definitions and Compliance]", public-tracking@w3.org mailing list, May 30, 2012, http://lists.w3.org/Archives/Public/public-tracking/2012May/0341.html.

[65] Bruce Yandle, "Bootleggers and Baptists-The Education of a Regulatory Economist," Regulation 7, no. 3 (1983): 12. http://www.cato.org/pubs/regulation/regv7n3/v7n3-3.pdf

Testimony of
Berin Szoka, President
TechFreedom[1]

on

"The Need for Privacy Protections: Is Industry Self-Regulation Adequate?"

Before the Senate Commerce Committee[2]
June 28, 2012

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison—thank you for inviting me to testify about privacy again before your Committee. As President of TechFreedom, a non-profit think tank, and before that, as Director of the Center for Internet Freedom at The Progress & Freedom Foundation, I have worked for over four years to articulate an alternative perspective on privacy that recognizes both the enormous value created by data and the need to prevent abuses of data. The debate thus far has systematically underestimated the benefits to consumers from the use of personal data to tailor advertising, develop new products, and conduct research, while overstating the dangers of data, which remain largely conjectural.

With the best of intentions, we are heading towards reshaping the fundamentals of the Internet—in ways that may have serious negative unintended consequences for privacy, the sites and services consumers enjoy, and the health of the ecosystem. But the *way* we're doing it may be even more troubling. This is not the result of a bottom-up evolutionary process, but of collusion between government and powerful market players. We are heading for opt-in dystopias.

II. The American Layered Approach to Privacy

I agree that self-regulation is not enough, that so-called "baseline" legislation is, indeed, necessary. I disagree, however, that *new* baseline legislation is needed. We already have baseline consumer protection legislation: Section V of the Federal Trade Commission Act[3] empowers the FTC not only to enforce self-regulation by holding companies to their promises,

---

1 Berin Szoka (@BerinSzoka) is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on consumer privacy. In particular, he testified on Balancing Privacy and Innovation before the House Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade on March 29, 2012, available at http://tch.fm/KCrz8k, ("Szoka Testimony").

2 http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=aa018084-ceea-472c-af63-97d7f44fac80.

3 15 U.S.C. § 45 (2006).

but also to prohibit as "unfair" uses of personal data that do more harm than good and that consumers themselves cannot reasonably avoid. States have similar legislation, empowering Attorneys General to act,[4] and class action lawsuits also deter privacy violations.[5]

On top of this baseline, we have built a layered approach to privacy protection. Where the FTC's authority has proven inadequate, Congress has enacted legislation to address specific problems, such as the Children's Online Privacy Protection Act[6] and the Fair Credit Reporting Act.[7] But in general, American law follows a common law model, addressing problems on a case by case basis rather than attempting to design a comprehensive regulatory scheme adequate for both present and future. This is what Richard Epstein famously called "Simple Rules for a Complex World."[8] The Electronic Frontier Foundation's Mike Godwin put it best in 1998 when he said: "It's easier to learn from history than it is to learn from the future. Almost always, the time-tested laws and legal principles we already have in place are more than adequate to address the new medium."[9]

Applying baseline principles of consumer protection is the best way to address new privacy challenges, given the ever-changing nature of the technologies involved and the inevitable trade-offs among competing conceptions of privacy, and between privacy and other values—such as:

- Funding for innovative media and services that would not otherwise be available;
- The diversity and competitiveness of an Internet ecosystem with low barriers to entry;
- The ease of use for consumers of an Internet that is not divided by checkpoints asking for consent or payment as users cross domain name boundaries;
- The innovation driven by discoveries made possible by analyzing what some have pejoratively labeled "Big Data," and so on.

Policymakers simply do not have the expertise or foresight to make complex rules to decide these trade-offs—or the time to become experts in complex technologies. So it is here that self-regulation plays a critical role in our layered approach to privacy. As the White House

---

4 Henry N. Butler & Joshua D. Wright, Are State Consumer Protection Acts Really Little-FTC Acts?, 63 Fla. L. Rev. 163, 165 (2011) (discussing state laws empowering attorneys general to "combat consumer fraud and other deceptive practices").

5 Glenn G. Lammi, "Thanks, Google Buzz: Class Action Lawyers Celebrate Impending Fees," Forbes,Nov. 3, 2010, available at http://www.forbes.com/sites/docket/2010/11/03/thanks-google-buzz-class-action-lawyers-celebrate-impending-fees/.

6 Children's Online Privacy Protection Act of 1998, Pub.L. No. 105-277, 112 Stat. 2581-728 (codified in 15 U.S.C. §§ 6501–6506).

7 Fair Credit Reporting Act of 1970, Pub. L. 91-508; 84 Stat. 1128 (codified in 15 U.S.C. § 1681).

8 Richard A. Epstein, Simple Rules for a Complex World (1995).

9 Quoted in Virginia Postrel, The Future and Its Enemies: The Growing Conflict Over Creativity, Enterprise, and Progress at 48 (Touchstone 1998).

privacy report acknowledged, self-regulation alone "can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges."[10]

In short, self-regulation is necessary, but not sufficient. It must work in tandem with the enforcement of existing laws—which I believe can be enhanced significantly *without* new legislation. But we must also understand that self-regulation is merely one part of a broader process by which market forces discipline corporations in how they collect, process, use and distribute personal data about us. Together, this layered approach is the best way to maximize the enormous benefits offered by the use of personal data while minimizing its occasional abuse.

III. Market Regulation of Privacy

Companies do not operate in a vacuum. They compete not just for customers, but to protect their good name in the eyes of business partners, shareholders, media watchdogs, potential employees, and citizens themselves. Nowhere in the economy is this more true than online, where companies compete both for consumers' attention and for the trust of business partners, especially advertisers.

The social media revolution has made it possible for anyone concerned about online privacy to blow the whistle on true privacy violations. That whistle may not always be loud enough to be heard, but it's more likely in this sector than any other. Traditional media sources like the Wall Street Journal have played a critical role in attracting attention to corporate privacy policies through "What They Know" series,[11] which has been popularized using social media tools. Reporters like Julia Angwin may rightly lament the failure of self-regulation in any particular case, but the very act of their criticism is essential for *market* regulation to function, because they are powerful actors in the marketplaces of ideas and reputation.

Earlier this year, social media tools were directed at Congress—to great effect—to express grassroots concern about the impact of proposed copyright legislation. While some Internet companies certainly helped to promote these messages, even were it not for their involvement, this experience would demonstrate how effective social media activism can be. There is no reason why such techniques cannot be used effectively against major Internet companies themselves, just as Facebook users have used Facebook itself to rally opposition to Facebook on privacy concerns such as its Beacon ad targeting system.[12] "The herd will be heard," as Bob

---

[10] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy at 23, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[11] *See generally What They Know*, Wall St. J., 2012, http://blogs.wsj.com/wtk/.

[12] See, e.g., Kirsten E. Marti, Facebook (A): Beacon and Privacy 3 (2010), available at http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf ("The online community responded immediately to this intrusion. MoveOn.org created a Facebook group "Petition: Facebook, stop invading my privacy!" that stated: "Sites like Facebook must respect my privacy. They should not tell my friends what I buy on other sites—or let companies use my name to endorse their

Garfield memorably put it in his 2009 book, *The Chaos Scenario: Amid the Ruins of Mass Media*.[13] The Choice for Business Is Stark: Listen or Perish. Among the most important factors driving companies to participate constructively in the multi-stakeholder process, to forge meaningful privacy protections, and to abide by them is the fear of a Wall Street Journal article, a social media frenzy, or organized campaign demanding action on a particular privacy problem.

As Wayne Crews of Competitive Enterprise Institute put it in testimony before this committee in 2008:

> Businesses are disciplined by responses of their competitors. Political regulation is premature; but "self-regulation" like that described in the FTC principles is a misnomer; it is competitive discipline that market processes impose on vendors. Nobody in a free market is so fortunate as to be able to "self regulate." Apart from the consumer rejection just noted, firms are regulated by the competitive threats posed by rivals, by Wall Street and intolerant investors, indeed by computer science itself.[14]

IV. Enhancing the American Layered Approach to Privacy

As I argued in March in testimony before the House Energy & Commerce Committee's Subcommittee on Commerce & Manufacturing,[15] the FTC could do much more with its existing authority to build an effective quasi-common law of privacy in three ways.

First, Congress should assess whether the FTC has adequate institutional resources and expertise. If the FTC had heeded my fellow panelist Peter Swire's call for the FTC to build a an office of information technology five years ago,[16] our layered privacy approach would today be far more effective in protecting consumers and ensuring their trust, and less easily dismissed as inadequate by foreign privacy regulators. Chairman Leibowitz deserves credit for appointing the agency's first Chief Technologist. But even with someone as talented as Ed Felten in that position, the FTC is still way behind the curve: His title is not Chief Technology *Officer* because there is no office behind him.

---

products—without my explicit permission." The Facebook group and petition had 2,000 members within the first 24 hours and eventually grew to over 80,000 names." [internal citations omitted]).

[13] James Cherkoff, "The Joy of a Gated Community," The Chaos Scenario, June 1, 2010, http://thechaosscenario.net/.

[14] Wayne Crews, Testimony Before the Senate Committee on Commerce, July 9, 2008, *available a*t http://cei.org/sites/default/files/Wayne%20Crews%20-%20Senate%20Commerce%20Testimony%20-%20Online%20Advertising,%20July%209%202008.pdf.

[15] Berin Szoka, Testimony Before the House Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade, "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?", Mar. 29, 2012, available at http://techfreedom.org/sites/default/files/Szoka%20Privacy%20Testimony%20to%20CMT%203.29.12%20v3%20(final)_0.pdf.

[16] Peter Swire, *Funding the FTC: Globalization and New Information Technologies Necessitate an Appropriations Boost*, Feb. 26, 2007, http://www.americanprogress.org/issues/2007/02/ftc.html.

The FTC needs a clear strategic plan outlining (a) how to build the in-house technical expertise it needs (beyond basic IT infrastructure) to identify enforcement actions, support successful litigation, monitor compliance, and conduct long-term planning and policy work, and (b) the resources necessary to achieve that goal through a combination of re-prioritizing current agency spending and additional appropriations. Importantly, this organization should function as a cohesive team that meets the needs for technical expertise of all the FTC's bureaus and offices (including the Bureau of Competition). A stand-alone organization could, like the Bureau of Economics, better attract and retain talent.

Second, the clearer privacy promises are, the more easily the FTC will be able to enforce them. One important way to achieve this goal would be for the FTC to promote the use of "smart disclosure"—the term used by Cass Sunstein, director of the Office of Information and Regulatory Affairs and a close advisor to President Obama, and a widely respected thinker in law, policy and technology. Smart disclosure can empower consumers by letting software do the work for them of reading privacy policies—and then implement their privacy preferences.

For example, users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app acedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct. As the FTC Privacy Report notes, smart disclosure could also "give consumers the ability to compare privacy practices among different companies."[17] An app store might illustrate how such comparisons could work, allowing users trying to choose between several competing apps to compare their privacy practices side by side.

While it would be preferable for smart disclosure to arise through self-regulation, especially given the complexity of crafting disclosure formats, mandating disclosure of privacy practices would generally be a better way for government to address demonstrated market failures than by dictating what constitutes fair information practices—and thus might be an appropriate area for Congress to explore legislation at some point.

Third, the proper measure of the FTC's effectiveness is not how many suits it successfully settles, but how well it contributes to the development of a quasi-common law of privacy that can guide companies pushing the envelope with new data-driven technologies—without stifling innovation that ultimately serves consumers. The chief problem today is that companies have only FTC complaints and consent decrees to guide in predicting the course of the law. These documents offer very little explanation of how the facts of a particular case satisfy the FTC's Policy Statements on unfairness and deception. And these summary assertions are never

---

[17] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 62 ("FTC Report"), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

tested in court, both because of the cost of litigation relative to settlement, and because of the cost to a defendant company of bad publicity from being perceived as anti-privacy exceed the benefits of taking the FTC to court—even when they would likely prevail given the FTC's overreach. While this should reassure us that reputation markets exert far greater pressure to discipline companies on privacy than is commonly appreciated, it also means that we lack the key ingredient for building a true common law: judicial scrutiny in an adversarial process.

The forces that keep privacy adjudication out of the courts and prevent development of privacy common law by judges are not likely to be easily overcome by FTC—or even Congressional—action. So we need to find alternative ways to replicate the adversarial process of careful analysis by which courts build upon simple rules to address the challenges of a complex world. I suggest the following six possible ways for the FTC to make better use of its existing authority to build a quasi common law:

1. The Commission (or individual Commissioners) should provide greater analysis of its rationale under its Unfairness and Deception Policy Statements for issuing each consent decree.
2. The FTC should, when it closes an investigation by deciding *not* to bring a complaint, issue a "no action" letter explaining why it decided the practice at issue was lawful under Section V.[18] Such letters, issued by other agencies like the Securities and Exchange Commission, provide an invaluable source of guidance to innovators. Congress should even consider whether the FTC should be required to issue such letters.
3. The FTC should consider how it could use advisory opinions more effectively to provide guidance to industry on how the agency might evaluate new privacy practices—especially for companies working on the cutting edge of technology, which are often small. The FTC issues such letters on a wide range of topics,[19] yet does not appear to have issued advisory opinions regarding the application of Section V to privacy.
4. Congress should reassert the vital oversight it exercised in 1980 and 1983 when it ordered the agency to issue the Policy Statements on Unfairness and Deception. At a minimum, the FTC should be required to explain, in detailed analysis, how it has applied those venerable standards in past privacy enforcement cases, and how it plans to do so in the future—again, because it is "easier to learn from history than it is to learn from the future."[20] Such guidelines are routine in other areas, and provided for in the

---

[18] *See, e.g.,* Jodie Bernstein, *Re: Petition Requesting Investigation of, and Enforcement Action Against SpectraCom, Inc.*, http://www.ftc.gov/os/1997/07/cenmed.htm.

[19] 16 C.F.R .§ 1.1 (2012) ("Any person, partnership, or corporation may request advice from the Commission with respect to a course of action which the requesting party proposes to pursue. The Commission will consider such requests for advice and inform the requesting party of the Commission's views, where practicable, under the following circumstances... (1) The matter involves a substantial or novel question of fact or law and there is no clear Commission or court precedent; or (2) The subject matter of the request and consequent publication of Commission advice is of significant public interest."); *see also* Judith A. Moreland, *Overview of the Advisory Opinion Process at the Federal Trade Commission*, *available at* http://www.ftc.gov/bc/speech2.shtm.

[20] *See supra* note 9.

Commission's current procedures.[21] Indeed, the antitrust guidelines issued by the FTC and DOJ form a key element of the American common law of competition. The FTC has issued a number of Guides[22] to explain its approach to consumer protection—but none for consumer privacy.[23] The FTC's recently issued privacy report is no substitute for such a Guide—indeed, it has little grounding in the twin Policy Statements that are supposed to be the FTC's lodestars. To replicate some of the adversarial nature of actual litigation, the process must be the result of a substantive dialogue with affected stakeholders, and it must be subject to involved oversight from the full Commission and from Congress.

5. In particular, the FTC must clarify the boundaries of privacy harm under the Unfairness Doctrine. The FTC's leadership seems to to be trying to have it both ways: playing down publicly what they can do with their existing legal authority (to support their argument for new statutory authority) while, at the same time, making bold claims about the scope of harm in their enforcement actions. If the concept of harm is stretched too far, the Unfairness Doctrine will become again, as it was in the 1970s, a blank check for the FTC to become a second national legislature.[24] I explain my concerns about the potential for the unfairness doctrine to be abused, but also my belief that the doctrine should be used to the greatest extent degree with the 1980 Policy Statement, in my March testimony before the House Energy & Commerce Committee.[25]
6. Congress should ensure the FTC has the resources adequate to engage in this detailed analysis. To dismiss the current legal model as inadequate simply because it has not been fully utilized, and to adopt instead a new legislative framework whose true costs are unknown, would be truly "penny wise, pound foolish." Given the clear need to reduce federal spending across the board, and the decidedly mixed record of antitrust law in actually serving consumers, Congress could simply reallocate funding from the FTC's Bureau of Competition—or, more dramatically, consolidate antitrust enforcement at the DOJ and allocate the cost savings from streamlining to the FTC's Bureau of Consumer Protection.[26]

If Congress wants to improve upon the American layered approach to privacy, these suggestions offer concrete steps that could be taken today. Just as Silicon Valley's motto is "Iterate, iterate, iterate," the same approach is needed for improving our existing framework.

---

[21] Federal Trade Comm'n, FTC Operating Manual §8, *available at* http://www.ftc.gov/foia/ch08industryguidance.pdf.

[22] Federal Trade Comm'n, FTC Bureau of Consumer Protection - Resources: Guidance Documents, http://ftc.gov/bcp/menus/resources/guidance.shtm (last visited June 26, 2012).

[23] Federal Trade Comm'n, Legal Resources | BCP Business Center, http://business.ftc.gov/legal-resources/48/33 (last visited June 26, 2012).

[24] See generally, Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, § III, http://www.ftc.gov/speeches/beales/unfair0603.shtm [hereinafter *Beales Paper*]).

[25] *See* Szoka, *supra* at 15.

[26] See William E. Kovacic, The Institutions of Antitrust Law: How Structure Shapes Substance, 110 Mich. L. Rev. 1019, 1034 (2012) (identifying several problems with federal duality of antitrust jurisdiction).

Only by using the current framework to its fullest capacity will we actually know if there are real gaps the FTC cannot address using its existing authority. In particular, the process of issuing guidelines could identify problems as candidates for appropriately narrow legislation that could build on top of the current baseline as part of an effective layered approach—or for self-regulatory processes akin to those called for by the NTIA. If there are some forms of harm that require government intervention but that cannot fit within an appropriately limited conception of harm under unfairness, it may be better for Congress to address these through carefully tailored legislation, rather than shoehorning them into unfairness. For example, such legislation might be appropriate to prevent employers from pressuring employees into sharing their passwords to Facebook and other social networking sites.

V. The DAA: A Self-Regulatory Success Story

The Digital Advertising Alliance has demonstrated how self-regulation can evolve to provide "the flexibility, speed, and decentralization necessary to address Internet policy challenges"—not perfectly, but better than government. Since my fellow witness Bob Liodice, is representing the DAA today, let me just highlight four areas in which I think DAA has demonstrated the value of self-regulation beyond its additional principles:

- **Transparency**: In April 2010, the industry began including an icon inside targeted ads to raise awareness of the practice and offer consumers an easy opt-out from tailored advertising. That icon is now shown in over a trillion ad impressions each month.
- **Education**: Last January, DAA launched an unprecedented public awareness campaign called "Your AdChoices" to further increase public awareness of the AdChoices Icon, and consumers' ability to opt-out.
- **Evolving commitments**: In November 2011, the DAA updated its principles to bar data collected for advertising purposes from being used for employment, credit, health care treatment, or insurance eligibility decisions.[27]
- **Enforcement**: The Better Business Bureau, which administers enforcement of the DAA principles, and has done so for other self-regulatory programs since 1971, has brought a number of enforcement actions,[28] demonstrating that it is far from toothless.
- **Do Not Track**: In February, the DAA committed[29] to respect Do Not Track (DNT) headers sent by browsers when users visit websites as a (potentially) more consumer-friendly way of implementing DAA's existing privacy opt-out.

---

[27] Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data, Nov. 2011, http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[28] See Better Business Bureau, Case Decisions, http://www.bbb.org/us/interest-based-advertising/decisions/ (last visited June 26, 2012).

[29] Digital Advertising Alliance, DAA Position on Browser Based Choice Mechanism, Feb. 22, 2012, http://www.aboutads.info/resource/download/DAA_Commitment.pdf.

VI. Concerns about Self-Regulatory Processes

The DAA is a good example of self-regulation evolving. But not all self-regulation is created equal. I have previously outlined my concerns about the self-regulatory process the NTIA has proposed to facilitate.[30] Chief among those concerns was the role government play in steering the process through the exercise of "soft power." My participation in the World Wide Web Consortium (W3C) process as an invited expert (for the last six weeks) has increased that concern dramatically, given the looming presence of the FTC, and to a lesser extent, European governments, behind that process. In particular, I fear that an artificial deadline imposed by the FTC and other global regulators may shape the outcome of the process in ways that prove counter-productive.

More generally, despite my general skepticism of antitrust and belief that market power is best combated with market power, my experience with W3C has made me appreciate better the concerns raised by FCC Commissioner Tom Rosch about manipulation of the self-regulatory process by powerful players—especially where market power is essentially piggybacking on the soft power of government. In his dissent from the FTC's 2012 privacy report, Rosch asked: "the major browser firms' interest in developing Do Not Track mechanisms begs the question of whether and to what extent those major browser firms will act strategically and opportunistically (to use privacy to protect their own entrenched interests)."[31] And in his concurrence to the draft version of that report released in December 2010, Rosch noted: "the self-regulation that is championed in this area may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power."[32]

These concerns about power are heightened by concerns about process. The W3C is highly respected as a standard-setting body, but it is not a *policy*-making body. Its first and only other policy-heavy process—to produce the Protocol for Privacy Preferences (P3P), a laudable but highly complex form of smart disclosure—was roundly criticized and never achieved widespread adoption.

Many key players are simply not represented—most notably the publishers, smaller advertising companies and data processors. All of these have a great deal to lose and could be put out of business, or forced to consolidate with larger players, in a Default DNT-On world. In large part,

---

[30] Berin Szoka, Comments to the National Telecommunications and Information Administration on the Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, April 2, 2012, http://techfreedom.org/sites/default/files/Comments%20to%20NTIA%20on%20Self-Regulatory%20Process%204.2.12.pdf.

[31] Dissenting Statement of Commissioner J. Thomas Rosch, Issuance of Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Mar. 26, 2012, at 6, *available at* http://www.ftc.gov/speeches/rosch/120326privacyreport.pdf.

[32] Concurring Statement of Commissioner J. Thomas Rosch, Issuance of Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Dec. 1, 2010, at E-3, *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

this reflects the high cost of participation, not just in terms of W3C membership,[33] but in terms of committing at least one person to engage in the weekly teleconference, the deluge of emails on the discussion list and the face-to-face meetings, which run 2.5 days.

It is also possible that the W3C Tracking Protection Working Group, while composed of talented, well-meaning and dedicated people, may simply not reflect the right mix of backgrounds, even among the companies represented. Significantly under-represented are those who could speak with authority to the real world trade-offs inherent in the many complicated decisions being made by the group—not enough business experts, no economists, and too many privacy advocates full of good intentions but lacking in real-world grounding. The stakes could scarcely be higher, with regulator standing ready to implement the outcome of the process, regardless of whether it is well-suited to the problems at hand.

Further, the process has proven highly unwieldy, given the large number of people involved and the large policy implications of the questions being debated—which were amplified considerably by Microsoft's decision to switch to Default DNT-On.

Still, for all its flaws, it may prove—to paraphrase Winston Churchill on democracy—that the W3C process is the worst possible process—except for all the others. Certainly, it is a better option than having the FTC design a DNT mechanism on its own, as has been proposed in pending legislation.[34]

I explain all these concerns in more detail below.

VII. The Dangers of Default DNT-On

Default DNT-On is supposed to empower users but in fact, it simply empowers browser makers to force a fundamental change in the Internet ecosystem, from today's low-friction, flat ecosystem of independent sites and services funded by impersonal data collection to one with fewer players who collect more data—"opt-in dystopias."

Since last September, the W3C has been developing a technical standard for Do Not Track (DNT) headers that would "allow a user to express their personal preference regarding cross-site tracking." The W3C process was based on the idea that the DNT mechanism "must reflect the user's preference." Similarly, the DAA commitment was premised on the idea that the user has "affirmatively chosen to exercise a uniform choice with the browser based tool."[35] Simply put, users, not browsers, should choose to opt-out of the data collection that creates so much value for consumers.

---

[33] A US company with over $50 million in annual revenue must pay $68,500/year, while smaller companies must pay $7900, and startups with fewer than ten employees and $3 million in annual revenue pay $2250. W3C, Membership Fees, http://www.w3.org/Consortium/fees?country=United+States&quarter=04-01&year=2012#results (last visited June 26, 2012).

[34] H.R. 654, Do Not Track Me Online Act, available at http://hdl.loc.gov/loc.uscongress/legislation.112hr654.

[35] Digital Advertising Alliance, *supra* note 27.

Microsoft breached this consensus on user choice when it announced last month that its new IE10 browser would send DNT:1 headers by default. This risks derailing the entire W3C process. Just the day before Microsoft's announcement, at the weekly W3C teleconference, privacy researcher Lauren Gelman attempted to allay industry concerns that the spec might go too far by saying: "realistically, majority default DNT is not the world this standard will exist in. DNT is going to be a 10% solution"[36]—a view overwhelmingly shared by participants.

While Microsoft's stated commitment to user empowerment is laudable, Default DNT-On doesn't empower users any more than turning on ad blocking by default would. Anyone who cares can quite easily choose to make that choice. Below a certain threshold of DNT adoption, few sites will find it worthwhile to charge, block or negotiate with those privacy-sensitive users who turn on DNT. But no-cost opt-outs and implicit *quid pro quos* don't scale: beyond a certain point, sites will have to make *quid pro quos* explicit to gain opt-ins (technically, exceptions to DNT). In other words, a significantly higher DNT adoption rate will take us past a tipping point to an opt-in world.

Some downplay the significance of this change, arguing that Default DNT-On will simply force negotiations between sites and users over granting exceptions[37]—a key part of the DNT spec. But as I explained in my comments on the draft FTC privacy report in February 2011, such negotiations are not costless; they introduce considerable transactions costs ("friction") into an ecosystem that currently works because it generated tiny amounts of value from enormous volumes of transactions. Economic theory suggests that forcing today's implicit quid pro quo to become explicit (by switching to DNT Default-On) could produce dramatically different outcomes. As I explained:

> Much as I enjoy the rich irony of seeing those who are rarely thought of as free-marketeers essentially asserting that "markets" will simply, and quickly, "figure it out," I am less sanguine. The hallmark of a true free-marketeer is not a belief that markets work perfectly; indeed, it is precisely the opposite: an understanding that "failure" occurs all the time, but that government failure is generally worse, in terms of its full consequences, than "market" failure.[38]

The first part of that lesson comes especially from the work of the economist Ronald Coase... who won his Nobel Prize for explaining that the way property rights are allocated and markets

---

[36] *See* Lauren Gelman, "Re: tracking-ISSUE-150: DNT conflicts from multiple user agents [Tracking Definitions and Compliance]", public-tracking@w3.org mailing list, May 30, 2012, http://lists.w3.org/Archives/Public/public-tracking/2012May/0341.html.

[37] Jonathan Mayer, "Do Not Track Is No Threat to Ad-Supported Businesses," Jan. 20, 2011, http://cyberlaw.stanford.edu/node/6592.

[38] Comments of Berin Szoka, on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, A Preliminary FTC Staff Report of the Bureau of Consumer Protection, Federal Trade Commission, February 18, 2011, http://techfreedom.org/sites/default/files/TechFreedom%20FTC%20filing%202011-02-18.pdf

are structured determines the outcome of marketplace transactions.[39] For example, a rule that farmers bear the cost of stopping rancher's cattle from grazing on their farms by constructing fences will produce different outcomes—not merely different allocations of costs—from the opposite rule.

Coase's key insight was that, in a perfectly efficient market, the outcome would not depend upon such rules: To put this in terms of the privacy debate, the choice between, say, an opt-out rule and an opt-in rule for the collection or use of a particular kind of data (essentially a property right) would have no consequence because the parties to the transaction (say, website users and website owners) would express their "true" preferences perfectly, effortlessly and costlessly. But, of course, such frictionless nirvanas do not exist. The real world is defined by what Coase called "transactions costs": search and information costs, bargaining and decision costs, policing and enforcement costs.

The transaction costs of implementing a "Do Not Track" mechanism above an acceptable loss threshold of adoption—where sites must create architectures of negotiation—are considerable: someone must design interfaces that make it clear to the user what their choice means, the user must consume that information and make a choice about tracking, websites must decide how to respond to various possible choices and be able to respond to users in various ways through an interface that is intelligible to users, and so on—all for what might seem like a "simple" negotiation to take place.

These problems are certainly not insurmountable—and, again, with the right engineering and thoughtful user interface design a "Do Not Track" mechanism could well prove a useful tool for expressing user choice. But when we look at the world through Coase's eyes, we begin to understand how mechanism design can radically alter outcomes (in this case, funding for websites).

Put simply, Default DNT-On could take us from a world in which users can freely browse content and services offered by a thriving ecosystem of publishers to a bordered Internet. Users will either have to pay or opt-in to tracking. In this worst-case opt-in "dystopia," consumers could be made significantly worse off in three primary ways.

First, to the extent publishers have to rely on micropayments or subscriptions, their revenues will likely drop. Information goods have a marginal cost of zero, and therefore competition tends to drive their marginal cost to zero. Put more simply: unless you have a unique good protected by copyright, it's hard to charge for it (and charging for many small transactions itself creates high transactions costs). Advertising has always solved this problem by monetizing attention, but advertising online is worth three or more times more when it is tailored to users'

[39] Ronald A. Coase, The Problem of Social Cost, 3 J.L. & Econ. 1 (1960).

interests.[40] Many sites that rely on this revenue will simply disappear, or be consolidated into larger media companies. Consumers will have fewer, poorer choices.

Second, those sites and data companies that are able to obtain opt-ins will likely collect *more* data in ways that are more personal than today. While opt-ins sound great in theory, they simply do not protect privacy in the real world. As Betsy Masiello and Nicklas Lundblad explained in their seminal paper about "Opt-In Dystopias":

> opt-in regimes … are invasive and costly for the user and can encourage service providers to minimise the number of times opt-in is requested. This can have at least two adverse effects.
>
> The first is that service providers may attempt to maximise data collection in every instance that they are forced to use an opt-in framework; once a user consents to data collection, why not collect as much as possible? And the increased transaction costs associated with opt-in will lead service providers to minimise the number of times they request opt-in consent. In combination these two behaviours are likely to lead to an excessive scope for opt-in agreements. In turn, users will face more complex decisions as they decide whether or not to participate. [41]

The DNT spec allows sites to negotiate with users to grant exceptions to DNT as an explicit *quid pro quo* for access to content or services. But this could rapidly become complex given the need for users to manage exceptions for multiple sites and services:

> As this happens we are likely to see demand rise for single identity systems.... It is possible that emerging social web services could comply by setting up the opt-in as a part of the account registration process, as discussed earlier. Users have an incentive to opt-in because they want to evaluate the service; after opting-in, a user is able to make an evaluation of the service, but by that point has already completed the negotiation. The service, having already acquired the mandatory opt-in consent, has no incentive to enable users to renegotiate their choice.
>
> The data collection in this instance would all be tied to a central identity and would be likely to have excessive scope and deep use conditions. One unintended consequence of a mandatory opt-in regime might be the emergence of tethered identities, whereby a user's identity is tightly coupled with a particular social platform or service.…
>
> From a privacy point of view, tethered identities present many challenges. The concept suggests that all behaviour is tied to a single entry in a database. The

---

[40] See, Howard Beales, *The Value of Behavioral Targeting*, March 2010, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

[41] N Lundblad and B Masiello, "Opt-in Dystopias", (2010) 7:1 SCRIPTed 155, http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

> ease of executing an overly broad law enforcement request would be far greater than in a regime of fragmented and unauthenticated data collection. The degree of behaviour upon which an advertisement might be targeted would also be far greater. And the threat of exposure posed by a security breach would also increase.

Third, few publishers and data-driven companies will be able to obtain opt-in exceptions to DNT. This will force unprecedented consolidation in the Internet ecosystem, both among publishers and among companies that use and process data for advertising, research and other purposes. As Masiello and Lundblad explain:

> A worst-case consequence of widespread opt-in models would be the balkanisation of the web. As already discussed, some degree of data collection is necessary to run many of today's leading web services. Those that require account registration, such as social web services, enjoy an easy mechanism for securing opt-in consent and would be likely to benefit disproportionately from a mandatory opt-in policy.
>
> If we believe that mandatory opt-in policies would disproportionately benefit authenticated services, we might also expect balkanisation of these services to occur. When information services are open and based on opt-out, there are incentives to provide users the best experience possible or they will take their information elsewhere. When these services are closed and based on opt-in, there are incentives to induce lock-in to prevent users from switching services. Users might be reluctant to leave a service they have evaluated and invested in; the more investment made the more likely a user is to stay with the current provider. We might expect mobility to decrease, with negative effects for competition and consumer value

Simply put, Default DNT-On is likely to drive the adoption of federated content networks, and the evolution of highly decentralized web sites and services towards an apps based model—such as on mobile phones and such as Microsoft is introducing in Windows 8—in which advertising is delivered by the app platform operator. This might or might be a good thing on net, but again, the point is that no one really knows, even as we tumble blindly down this path.

With the best of intentions, we are heading towards reshaping the fundamentals of the Internet—in ways that may have serious negative unintended consequences for privacy, the sites and services consumers enjoy, and the health of the ecosystem. But the *way* we're doing it may be even more troubling. This is not the result of a bottom-up evolutionary process, but of collusion between government and powerful market players. In the name of self-regulation, we are essentially moving toward the European model of co-regulation: where governments steer and industry rows, and where powerful incumbents use market power to serve their own agendas, with the blessing of government.

The Federal Trade Commission called for a Do Not Track mechanism in its draft privacy report, issued in December 2010. Chairman Leibowitz and David Vladeck, Director of the FTC's Bureau

of Consumer Protection, have taken credit for pressuring industry to come to the table on DNT.[42] The agency has played an active role in the W3C process. FTC Chief Technologist Ed Felten opened day two of the most recent W3C meeting by telling participants what the FTC wanted. Chairman Leibowitz and Commissioner Julie Brill delivered keynote addresses at the two prior meetings. Commissioner Brill, in particular, has pushed the W3C process to change the nature of the DNT spec to limit not just how data can be used, but what data can be collected in the first place. Representatives Ed Markey and Joe Barton have gone even further, sending a letter to the W3C Tracking Protection Working Group during its last meeting urging not only heavy restrictions on collection, but also that DNT:1 be turned on default.[43]

The FTC has clearly been turning the screws on companies to agree to comply with DNT—even before a standard exists. The FTC showed its hand in Twitter's agreement to recognize DNT in May,[44] when FTC Chief Technologist Ed Felten announced the deal himself even before Twitter could do so. Faced with the FTC's open antitrust investigation, and the agency's essentially unchecked ability to bring privacy complaints against the company, at a real cost to its reputation, it's not hard to see why Twitter might be susceptible to... encouragement from the well-meaning folks at the FTC.

So one has to wonder what role Chairman Leibowitz, and members of Congress like Representatives Barton and Markey, might have had in convincing Microsoft to break ranks from the W3C process—even if that risked derailing the process itself.

This is, of course, speculative—but not without any basis. At the very least, Congress should ask the FTC to explain exactly what its role has been throughout this process. Further, Congress should call on the agency's leadership to repudiate the disturbing argument made by Tim Wu in defense of "agency threats" as a valid form of extra-legal regulation.

VIII. Conclusion

There are no silver bullets. Neither self-regulation nor relying on Section V is without pitfalls. But together, and working in conjunction with market forces like reputation, with targeted legislative solutions, and with technological change itself, they form a layered approach to dealing with privacy that is more likely to protect us from true privacy harms without killing the goose that laid the golden egg.

---

[42] Federal Trade Commission, FTC Testifies on Do Not Track Legislation, Dec. 2, 2010, http://www.ftc.gov/opa/2010/12/dnttestimony.shtm.

[43] Letter from Congressmen Edward J. Markey and Joe Barton to World Wide Web Consortium Tracking Protection Working Group, June 19, 2012, available at http://markey.house.gov/sites/markey.house.gov/files/documents/%206-19-12%20Letter%20from%20Rep%20Markey%20and%20Barton%20-%20W3C%20.pdf.

[44] Michelle Maltais, "Twitter supports 'do not track'", Los Angeles Times, May 17, 2012, available at http://articles.latimes.com/2012/may/17/business/la-fi-tn-twitter-do-not-track-20120517.

Humility, Institutional Constraints & Economic Rigor: Limiting the FTC's Consumer Protection Discretion

Geoffrey A. Manne
Executive Director,
International Center for Law & Economics

February 2014
Revised, July 2014

ICLE Antitrust & Consumer Protection Program Working Paper 2014-1

ICLE | 2325 E Burnside Street, Suite 301 | Portland, OR 97214 | 503.770.0652
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

Humility, Institutional Constraints & Economic Rigor: Limiting the FTC's Consumer Protection Discretion

Geoffrey A. Manne, International Center for Law & Economics

ICLE | 2325 E Burnside Street, Suite 301 | Portland, OR 97214 | 503.770.0652
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

Introduction

In 1914, Congress gave the FTC sweeping jurisdiction and broad powers to enforce flexible rules, to ensure that it would have the ability to serve as the national regulator of trade and business. Much, perhaps even the great majority, of what the FTC does is uncontroversial and is widely supported, even by critics of the regulatory state. However, both Congress and the courts have expressed concern about how the FTC has used its considerable discretion in some areas. Now, as the agency approaches its 100th anniversary, the FTC, courts, and Congress face a series of decisions about how to apply or constrain that discretion. These questions will become especially pressing as the FTC uses its authority in new ways, expands its authority into new areas, or gains new authority from Congress (such as over data security or privacy).

The FTC oversees nearly every company in America. It polices competition by enforcing the antitrust laws. It also protects consumers by punishing deception and practices it deems "unfair." Under its consumer protection authority, it is the general enforcer of corporate promises made in privacy policies and codes of conduct generated by industry or multistakeholder processes. It is the de facto regulator of the media, from traditional advertising to Internet search and social networks. And it handles novel problems of privacy, data security, online child protection, and patent claims, among others. Even net neutrality may soon wind up in the FTC's jurisdiction.

The Federal *Technology* Commission

But perhaps most importantly, the Federal Trade Commission has become, for better or worse, the Federal *Technology* Commission. Technology creates a special problem for regulators.

Inherent limitations on anyone's knowledge about the future nature of technology, business and social norms caution skepticism as regulators attempt to predict whether any given business conduct will, on net, improve or harm consumer welfare. In fact, a host of factors suggests that even the best-intentioned regulators may tend toward overconfidence and the erroneous condemnation of novel conduct that benefits consumers in ways that are difficult for regulators to understand.[1] At the same time, business generally succeeds by trial-and-error more than theoretical insights or predictive power,[2] and over-regulation thus risks impairing

[1] *See*, *e.g.*, Ronald H. Coase, *Industrial Organization: A Proposal for Research*, *in* ECONOMIC RESEARCH: RETROSPECT AND PROSPECT VOL. 3: POLICY ISSUES AND RESEARCH OPPORTUNITIES IN INDUSTRIAL ORGANIZATION (Victor R. Fuchs, ed. 1972), *available at* http://www.nber.org/chapters/c7618.pdf; Frank H. Easterbrook, *The Limits of Antitrust*, 63 TEX. L. REV. 1 (1984); Geoffrey A. Manne & Joshua D. Wright, *Innovation and the Limits of Antitrust*, 6 J. COMPETITION L. & ECON. 153 (2010).

[2] *See* Armen Alchian, *Uncertainty, Evolution, and Economic Theory*, 58 J. POL. ECON. 211 (1950).

experimentation, an essential driver of economic progress. As a consequence, doing nothing may sometimes be the best policy for regulators, and limits on regulatory discretion to act can be of enormous importance.[3]

But technology does present unique—or perhaps just especially exigent—challenges for regulators precisely because it tends to create new consumer protection and competition issues, or upset previously settled issues, and because such change tends to occur more rapidly than in some other settings. Regulation abhors a vacuum; technology tends to render existing regulation obsolete, creating such a vacuum. Moreover, technology can give rise to *new* issues, or at least *new-seeming* issues, which can leave regulators looking for novel regulatory tools and justifications for regulation. That is, regulators often feel the need to do *something*, even where it is unclear whether or what regulation is needed.

It is on the cutting edge, new issues that the stress-points in the FTC's general approach become most clearly visible, but these stress-points are by no means unique to the technological setting. Moreover, of particular importance, welfare-enhancing innovation is not just about technological advance, but also organizational, business model and contractual developments, and these important advances can also be threatened by the excessive use of discretion.[4]

But it is in the realm of new technology that many of the FTC's most significant recent cases have arisen and such cases exemplify these concerns. Facing novel data security questions, the agency has pushed the bounds of its authority over unfair and deceptive acts and practices (UDAP)[5] to constrain firms trying to experiment and adapt in the face of developing technology. Similarly, by expressing myriad concerns about business methods and practices in high-tech firms—among them Intel, N-Data, Twitter, Google, Facebook Apple and Amazon—and investigating issues ranging from privacy to search engine design to patent enforcement to integrated circuit fabrication, the Commission has pushed the bounds of its Section 5 authority,[6] and has indicated its desire to continue expanding the power afforded by that

---

[3] As Nobel Laureate economist Ronald Coase put it, "direct governmental regulation will not necessarily give better results than leaving the problem to be solved by the market or the firm. But equally there is no reason why, on occasion, such governmental administrative regulation should not lead to an improvement in economic efficiency.... There is, of course, a further alternative which is to do nothing about the problem at all." Ronald H. Coase, *The Problem of Social Cost*, 3 J. LAW & ECON. 1, 18 (1960).

[4] *See, e.g.*, Manne & Wright, Innovation, *supra* note 1; ERNEST GELLHORN, & WILLIAM E. KOVACIC, ANALYTICAL APPROACHES AND INSTITUTIONAL PROCESSES FOR IMPLEMENTING COMPETITION POLICY REFORMS BY THE FEDERAL TRADE COMMISSION (Dec. 1995), *available at* http://www.ftc.gov/opp/global/gmu_1.shtm.

[5] The FTC is empowered to police, among other things, "unfair or deceptive acts or practices." 15 U.S.C. § 45(a)(4)(A).

[6] Federal Trade Commission Act, 38 Stat. 719 (codified at 15 U.S.C. § 45).

authority. In short, any large (that is, successful and innovative) firm operating in the technology sector, would be prudent to expect that today the FTC is investigating its business practices.

The FTC must always weigh the costs of intervention (and the costs of getting it wrong) against the costs of doing nothing. But what, and who, will limit the discretion of a majority of FTC Commissioners in assessing these trade-offs? It is the age-old question: *Who will watch the watchers?* In technology the question becomes, how should the FTC regulate technology? What's the right mix of the certainty businesses need and the flexibility technological progress demands?

One thing is certain: a top-down, administrative regulatory model of regulation is ill-suited for technology. The epitome of the traditional regulatory model is the FTC's chief rival: the FCC. The 1996 Telecom Act runs nearly 47,000 words—65 times longer than the Sherman Act, for example. The FCC writes tech-specific regulations before technology has even developed. Virginia Postrel's apt words in *The Future and Its Enemies* describes its mentality best:

> Technocrats are "for the future," but only if someone is in charge of making it turn out according to plan. They greet every new idea with a "yes, but," followed by legislation, regulation, and litigation.... By design, technocrats pick winners, establish standards, and impose a single set of values on the future.[7]

Economics at the FTC

The most important, most welfare-enhancing reform the FTC could undertake is to better incorporate sound economic- and evidence-based analysis in both its substantive decisions as well as in its process. While the FTC has a strong tradition of economics in its antitrust decision-making, its record in using economics in other areas is mixed (or at least opaque). Meanwhile, a review of some recent decisions at the agency suggests that the Commission is inconsistent in its application of economic principles.

To be sure, the economic tools that the FTC uses have developed over time. Merger law, for example, used to be about counting the number of firms on one's fingers. Now, we have much more advanced tools that help decision-makers (and economic actors) to identify actual competitive effects, and that better enable the Commission to distinguish between welfare-enhancing conduct and its close, anticompetitive cousins. But still those tools are not crystal balls, and they have their limitations. Essential to the proper application of economic analysis in FTC decision-making is the recognition of these limits and the resistance to the urge to go *beyond* what our tools can reasonably accomplish.

---

[7] VIRGINIA POSTREL, THE FUTURE AND ITS ENEMIES 50 (1998).

In what follows I discuss several important aspects of the FTC's process and substantive decision-making, particularly those that bear on its regulation of technology. In doing so, I assess the contribution (or lack thereof) of proper economic analysis to the Commission's decisions and how it has contributed and can better contribute to the Commission's goal of promoting consumer welfare.

In what follows I draw significantly on Commissioner Wright's decision-making (as well as some of that of fellow Commissioner Maureen Ohlhausen) to highlight the role of economics at the FTC. When Joshua Wright was sworn in as Commissioner at the FTC in early 2013, he became only the fourth economist to serve in that capacity and the first JD/PhD to do so. Over the course of his first year on the Commission he has remained resolute in his adherence to economic principles as a guide to his decision-making. As a result, his various speeches, statements and dissents present a foil—a steadfast baseline of economic analysis—against which to assess the Commission's recent work. For Wright,

> economics provides a framework to organize the way I think about issues beyond analyzing the competitive effects in a particular case, including, for example, rulemaking, the various policy issues facing the Commission, and how I weigh evidence relative to the burdens of proof and production. Almost all the decisions I make as a Commissioner are made through the lens of economics and marginal analysis because that is the way I have been taught to think.[8]

Wright's approach has often been adopted by the Commission (most notably under economically-minded past Chairmen like Tim Muris and Bill Kovacic). But, as I will discuss, there are some glaring exceptions, particularly in the FTC's consumer protection enforcement practices.

Competition

Particularly when it engages in competition enforcement and policymaking, the FTC's model is more evolutionary than regulatory. It builds flexible law that evolves alongside technology. The agency learns from, and adapts to, the ever-changing technological and business environments. The key (besides, obviously, the ability to understand technology) is economics. And the FTC has generally been at the forefront among the world's competition agencies in incorporating economics into its decisions.

---

[8] Interview with Joshua Wright, FTC Commissioner, ABA Antitrust Section, Economic Committee Newsletter, Winter 2014, vol. 13, p. 6, *available at* http://www.americanbar.org/content/dam/aba/publications/antitrust_law/at308000_newsletter_2014winter.authcheckdam.pdf.

At the same time, judicial decisions are generally well-grounded in economics, and this feeds back into the agency's enforcement actions. Antitrust law has become nearly synonymous with antitrust economics: both courts and agencies weigh the perils of both under- and over-enforcement in the face of unavoidable uncertainty about the future.

The incorporation of this approach to competition law by the courts and regulatory agencies began in the late 1970s with the Supreme Court's 1977 *GTE Sylvania* decision[9] and the important influence of Richard Posner's 1976 book, ANTITRUST LAW: AN ECONOMIC PERSPECTIVE,[10] and Robert Bork's 1978 book, THE ANTITRUST PARADOX. THE ANTITRUST PARADOX made the case that antitrust law should be based on rigorous economic analysis – and that the subject of that analysis should be protecting consumer welfare. Today the FTC (like the DOJ) incorporates economics into its competition-related Guidelines[11] and enforcement decisions and most cases are now decided by courts under a rule of reason standard – a standard under which plaintiffs generally face the burden of demonstrating that conduct harms consumers and courts weigh its likely costs against its benefits.

One of the central themes of the modern era of antitrust can be characterized as "regulatory humility": Regulators should intervene in markets only with great caution. Several reasons urge such caution. First, the regulator's natural inclination – in fact, his very job – is to regulate. This inclination on the regulator's part is compounded by the fact that, as Ronald Coase explained:

> If an economist finds something – a business practice of one sort or another – that he does not understand, he looks for a monopoly explanation. And as in this field we are very ignorant, the number of ununderstandable practices tends to be very large, and the reliance on a monopoly explanation, frequent.[12]

Second, the greatest pressure for regulatory intervention against a firm often comes from that firm's competitors, which seek to use regulation to benefit themselves (not consumers). Many antitrust practitioners refer to this as "the first rule of antitrust": competitor complaints indicate that the market is, in fact, competitive. Third, even where regulatory intervention may

---

[9] Continental TV., Inc. v. GTE Sylvania, Inc., 433 U.S. 36 (1977), *available at* https://supreme.justia.com/cases/federal/us/433/36/case.html.

[10] It is interesting to note that with the publication in 2001 of the second edition of Posner's book, he dropped the "An Economic Perspective" from the title in recognition that the economic approach to antitrust law was no longer merely a distinct "approach," but rather that "antitrust law" had become essentially coextensive with "antitrust law and economics."

[11] *See, e.g.*, United States Department of Justice, *Guidelines and Policy Statements* (last accessed Feb. 25, 2014), http://www.justice.gov/atr/public/guidelines/.

[12] Coase, *Industrial Organization*, *supra* note 1, at 67.

be justified, it is often not clear what intervention is appropriate to the harms, especially in markets characterized by rapid change or innovation. A significant portion of the of the 125-year history of antitrust regulation is a catalog of failure – efforts that too often harmed the very consumers they were meant to protect.[13]

Last, and perhaps most important, market forces often constrain harmful conduct more effectively than regulation. In competitive markets, a firm's competitors will respond to its conduct. In noncompetitive markets, the monopoly profits extracted by the malfeasant firm will attract entry by competitors eager to share in the surplus as well as a response from firms already in the market. Such market responses may not offer a perfect response to harmful conduct. But they need not be perfect to be preferable to regulation – only better than the also-imperfect regulatory alternative.[14] Given the possibility that seemingly harmful conduct may, in fact, not be harmful, the difficulty of remedying harmful conduct, and the possibility that the remedy could actually harm competition and consumers, it is frequently the case that regulatory inaction is preferable to ill-conceived regulation.

Generally, this approach to analyzing competition concerns is called the "error cost" framework. Such a framework seeks to balance the potential harms of false positives (erroneous intervention) and negatives (erroneous restraint) – so-called Type I and Type II errors – against the potential benefits of correct judgments.[15] The error cost approach has come to dominate antitrust over the past 40 years. There is, however, constant pressure for antitrust law to take a more aggressive stance towards potentially harmful conduct. Yet the courts have consistently held antitrust to the more circumspect approach advocated in THE ANTITRUST PARADOX.

Mergers: *Nielsen/Arbitron*

While the economic approach has come to dominate competition law in both the courts and at the agencies, there are important and troubling exceptions in both places. The FTC's consent order in the recent Nielsen/Arbitron merger offers a poignant example.

A properly circumspect, economic approach to analyzing the merger would have done many things, and some of them the FTC did. But essential to economic analysis of technology markets is a regulatory humility that recognizes that the *industry itself* is unaware of how its future will unfold, what technologies will disrupt it, what conduct will prove to be beneficial

---

[13] An important exception to this is straightforward cartel prosecution. As I use the term in this essay, "antitrust regulation" should be understood not to include straightforward cartel prosecution.

[14] *See* Coase, *The Problem of Social Cost*, *supra* note 3, at 17-18.

[15] *See, e.g.*, Manne & Wright, *Innovation*, *supra* note 1, at 158-63.

and what will prove to be harmful. Pre-judging the formation of entirely new markets and assuming technology-based market power in these markets is utterly inconsistent with a proper economic approach.

In *Nielsen/Arbitron*, Commissioner Wright wrote a powerful and important dissent[16] from the FTC's 2-1 (Commissioner Ohlhausen was recused from the matter) decision[17] to impose conditions on Nielsen's acquisition of Arbitron. Essential to Wright's dissent is the absence of any actual existing market supporting the Commission's challenge:

> Nielsen and Arbitron do not currently compete in the sale of national syndicated cross-platform audience measurement services. In fact, there is no commercially available national syndicated cross-platform audience measurement service today. The Commission thus challenges the proposed transaction based upon what must be acknowledged as a novel theory—that is, that the merger will substantially lessen competition in a market that does not today exist.
>
> * * *
>
> [W]e…do not know how the market will evolve, what other potential competitors might exist, and whether and to what extent these competitors might impose competitive constraints upon the parties
>
> * * *
>
> To be clear, I do not base my disagreement with the Commission today on the possibility that the potential efficiencies arising from the transaction would offset any anticompetitive effect. As discussed above, I find no reason to believe the transaction is likely to substantially lessen competition because the evidence does not support the conclusion that it is likely to generate anticompetitive effects in the alleged relevant market.[18]

The theory put forward by the Commission is the kind of speculative theory that seriously threatens innovation. Regulators are singularly ill-positioned to predict the course of technological evolution — that's why they're not also billionaire innovators. To impose antitrust-based constraints on economic activity *that hasn't yet been contemplated* is directly at odds with a sensible, evidence-based approach to enforcement. It is also of a piece with the

---

[16] In the Matter of Nielson Holdings, NV and Arbitron, Inc. (Sep. 20, 2013), http://www.ftc.gov/os/caselist/1310058/130920nielsenarbitron-jdwstmt.pdf (Commissioner Wright, dissenting) [hereinafter "*Nielsen* Dissent"].

[17] Complaint & Consent, In the Matter of Nielson Holdings, NV and Arbitron, Inc. (Jan. 24, 2014), http://www.ftc.gov/os/caselist/1310058/index.shtm.

[18] Wright, *Nielsen* Dissent, *supra* note 16, at 5-6.

technocratic mindset Postrel criticizes (and which, it should be again noted, is not the norm for the FTC):

> For technocrats, a kaleidoscope of trial-and-error innovation is not enough; decentralized experiments lack coherence. "Today, we have an opportunity to shape technology," wrote [Newt] Gingrich in classic technocratic style. His message was that computer technology is too important to be left to hackers, hobbyists, entrepreneurs, venture capitalists, and computer buyers. "We" must shape it into a "coherent picture." That is the technocratic notion of progress: Decide on the one best way, make a plan, and stick to it.[19]

It should go without saying that this is the antithesis of the environment most conducive to economic advancement. Whatever antitrust's role in regulating technology markets, it must be evidence-based, grounded in economics and aware of its own limitations.

The economic problems with such conduct are considerable, as Commissioner Wright notes:

> A future market case, such as the one alleged by the Commission today, presents a number of unique challenges not confronted in a typical merger review or even in "actual potential competition" cases. For instance, it is inherently more difficult in future market cases to define properly the relevant product market, to identify likely buyers and sellers, to estimate cross-elasticities of demand or understand on a more qualitative level potential product substitutability, and to ascertain the set of potential entrants and their likely incentives. Although all merger review necessarily is forward looking, it is an exceedingly difficult task to predict the competitive effects of a transaction where there is insufficient evidence to reliably answer these basic questions upon which proper merger analysis is based.
>
> * * *
>
> When the Commission's antitrust analysis comes unmoored from such fact-based inquiry, tethered tightly to robust economic theory, there is a more significant risk that non-economic considerations, intuition, and policy preferences influence the outcome of cases.[20]

As Wright notes, facts are essential, but they are not enough. Particularly when predicting future effects, proper, restrained application of *economic rigor* to the facts is essential. And, as noted above, this entails a recognition of the limits of the regulator's (or anyone's) ability not only to *describe* the future, but to understand its competitive significance.

---

[19] VIRGINIA POSTREL, *supra* note 7, at 54.

[20] Wright, *Nielsen* Dissent, *supra* note 16, at 2, 3.

Thus, compare Commissioner's Wrights words about *Nielsen* with those of Deborah Feinstein, the FTC's current Director of the Bureau of Competition:

> The Commission based its decision not on crystal-ball gazing about what might happen, but on evidence from the merging firms about what they were doing and from customers about their expectations of those development plans. From this fact-based analysis, the Commission concluded that each company could be considered a likely future entrant, and that the elimination of the future offering of one would likely result in a lessening of competition.[21]

Instead of requiring rigorous economic analysis of the facts, for Feinstein the FTC fulfilled its mission in *Nielsen* by considering the "facts" alone (not *economic evidence*, but rather unreliable customer statements and expressions of intent by the parties) and then, at best, casually applying to them the simplistic, outdated structural presumption – the conclusion that increased concentration would lead inexorably to anticompetitive harm. Unfortunately, this mode of analysis underestimates the fragility of factual predictions about the future and elevates the resulting presumed descriptive clarity when it should be emphatically questioning it with more, not less, rigorous economic analysis.

The Use of "Hot Docs" and Intent Evidence

The FTC's antitrust cases and Guidelines have generally embraced sensible economic reasoning and been built largely on the basis of rigorous economic evidence. But even here its record is far from perfect, as its *Nielsen/Arbitron* consent order demonstrates. Instead, the FTC has often based its competition enforcement decisions not on economic evidence pointing to harmful outcomes, but on "hot docs" that purport to evince nefarious motives for challenged conduct – but that do not necessarily shed any light on actual competitive effects.

> This approach has a "the light's better over here" feel to it. It is undoubtedly easier to "discover" anticompetitive behavior and relevant markets by inferences from business language than it is to deduce it from rigorous economic analysis. Although it is not clear that this type of business rhetoric bears much relationship to economic reality, regulators and courts (to say nothing of juries) are moved by it nonetheless.[22]

---

[21] Deborah L. Feinstein, *The Forward-Looking Nature of Merger Analysis*, Speech given at Advanced Antitrust U.S. (2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/forward-looking-nature-merger-analysis/140206mergeranalysis-dlf.pdf.

[22] Geoffrey A. Manne & E. Marcellus Williamson, *Hot Docs vs. Cold Economics: The Use and Misuse of Business Documents in Antitrust Enforcement and Adjudication*, 47 ARIZ. L. REV. 609, 610-11 (2005).

Recently, the response from some former Commissioners to the DOJ's Section 2 Report,[23] as well as a series of speeches by former Commissioner Rosch,[24] indicate an alarming willingness to challenge the importance of economic evidence and economic analysis for the sake of winning cases. To the extent that, as a descriptive matter, economic evidence doesn't help win cases, the fault (if there is one) lies with the courts or with particular judges, not the Commission.

By contrast, however, where the Commission (or its Commissioners) *itself* embraces a diminished role for economic evidence, we should be concerned. The Bureau of Economics and other Commission staff provide economic, analytical inputs to the agency that should be deemed essential to making the right decision at the enforcement stage. The notion that *this* evidence should be disregarded is troubling.

As it happens, and as I've written about at length elsewhere, the non-economic evidence that apparently convinces trial judges can be harmful, imposing liability where the protection of consumer welfare demands permissiveness.[25] One of the important lessons of economics in antitrust is that economic tools are uniquely capable of distinguishing competitive from anticompetitive conduct — the perennial challenge of non-cartel antitrust enforcement and adjudication. There is no basis for the argument that, at the Commission level, we should be using less of our best tool because it is complicated and can involve Greek letters. As Commissioner Wright recently noted,

> In litigation, when you are in front of a judge, you have competing expert witness reports, and you have some hot docs. As a litigation strategy, it may be tempting to emphasize the documents because they are easier for the judge to understand than the standard errors of a regression. If that is true, then documents would tend to be over-emphasized in litigation.[26]

---

[23] Statement of Commissioners Harbour, Leibowitz and Rosch on the Issuance of the Section 2 Report by the Department of Justice (Aug. 9, 2008), http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-commissioners-react-department-justice-report-competition-monopoly-single-firm-conduct-under/080908section2stmt.pdf.

[24] J. Thomas Rosch, *Litigating Merger Challenges; Lessons Learned*, based on remarks given at the Bates White Fifth Annual Antitrust Conference (Jun. 2, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/litigating-merger-challenges-lessons-learned/080602litigatingmerger.pdf; J. Thomas Rosch, *Reactions on Procedure at the FTC*, remarks given at ABA Antitrust Masters Course IV (Sept. 25, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/reflections-procedure-federal-trade-commission/080925roschreflections.pdf.

[25] *See* Manne & Williamson, *Hot Docs*, *supra* note 22.

[26] Interview with Joshua Wright, *supra* note 8.

No doubt economists could be better at making their work accessible to a lay audience, including FTC Commissioners. But Commissioners at an expert antitrust agency have the responsibility and obligation to use all of the tools at their disposal not just to win cases, but first and foremost to understand the underlying economic issues that shed light on whether challenged conduct will harm or help consumers in practice. For instance, where economic analysis demonstrates that there is bad case law on the books that hasn't been overturned, there is a strong argument that, as an agency that provides a public good, the FTC should heed its economic wisdom and refrain from using such case law to win cases. The agency should also be concerned about making sure that competition law and policy develop correctly and in accordance with economic prescriptions, not just about winning cases at all costs.

But much non-economic evidence is counter-productive in this enterprise, tending to obscure rather than illuminate the competitive significance of ambiguous conduct:

> The problem is that these documents are easily misunderstood, and thus while the economic significance of such documents is often quite limited, their persuasive value is quite substantial. As one prominent accounting scholar notes, business documents and public filings containing accounting data "are useful for internal control, but are not designed or often useful for the measurements demanded by economists and lawyers."
>
> * * *
>
> To be sure, business documents can be appropriately useful to regulators in certain areas of inquiry. Business documents may be useful in providing data for economic analysis, and business documents also serve to provide a basic picture of the industry under scrutiny.
>
> On the other hand, some uses of these documents are simply inappropriate; in many cases, antitrust regulators and plaintiffs attribute unjustified economic and legal significance to the language of corporate managers. The consequence is that regulators and courts are writing out the economic underpinning of the antitrust laws and substituting rhetoric and unreliable accounting instead. This may lead to misguided enforcement that chills the competitive activity that antitrust is intended to foster.[27]

Intent evidence is similarly problematic:

> [U]nder some circumstances it makes sense for decision-makers to infer conduct from belief or intent…. But this inference is permissible only if there is truth to the underlying premise that an actor's intentions do, in fact, correlate with his actions. With respect to

[27] Manne & Williamson, *supra* note 22, at 612 (quoting George J. Benston, *Accounting Numbers and Economic Values*, 27 ANTITRUST BULL. 161, 162 (1982)).

> behavior subject to antitrust regulation, this is not necessarily the case. There is a significant distinction between the reliability of evidence used to demonstrate that an actor engaged in specific, intended conduct, and evidence used to demonstrate that an actor's conduct had a particular, economic, and legal effect.
>
> * * *
>
> The core problem is not that courts are unable to discern anticompetitive intent where it is present, nor even that they mistake procompetitive for anticompetitive intent (although these are problems, to be sure). Rather the problem is the fundamental and inextricable disconnect between intent and effect in complex economic systems.[28]

Or as one court put it:

> [A]n admitted intention to limit competition will not make illegal conduct that we know to be pro-competitive or otherwise immune from antitrust control. And, while "smoking gun" evidence of an intent to restrain competition remains relevant to the court's task of discerning the competitive consequences of a defendant's actions, "ambiguous indications of intent do not help us 'predict [the] consequences [of a defendant's acts]'" and are therefore of no value to a court analyzing a restraint under the rule of reason, where the court's ultimate role is to determine the net effects of those acts. Under such circumstances, we apply the rule of reason without engaging in the relatively fruitless inquiry into a defendant's intent.[29]

And as the court in *Microsoft* noted:

> [O]ur focus is upon the effect of that conduct, not upon the intent behind it. Evidence of the intent behind the conduct of a monopolist is relevant only to the extent it helps us understand the likely effect of the monopolist's conduct.[30]

Unfortunately, the Commission has shown a willingness to defer to intent evidence to make out (or define) anticompetitive conduct. In its statement closing its investigation into Google's search practices,[31] while the agency properly refrained from bringing a case, it nevertheless erred in some of its reasoning in getting there: Rather than focusing solely on Google's conduct and its anticompetitive effect, the FTC's statement also paid particular attention to Google's intent. Critics had contended that Google had engaged in conduct with exclusionary effect in

---

[28] *Id.* at 647-49.

[29] California Dental Ass'n v. FTC, 224 F.3d 942, 948 (9th Cir. 2000).

[30] United States v. Microsoft, 253 F.3d 34, 58-59 (D.C. Cir. 2001) (en banc).

[31] Federal Trade Commission, *Statement Regarding Google's Search Practices, In the Matter of Google Inc.*, at 3 (Jan. 3, 2013), *available at* http://www.ftc.gov/os/2013/01/130103googlesearchstmtofcomm.pdf.

search. But in the Commission's final ruling, there was no discussion of whether search bias (demoting a competitor in organic search results) actually constituted a refusal to deal. Rather, the discussion focused (appropriately) on effects and procompetitive justification, and (inappropriately) on Google's intent — but not on the nature of the conduct itself.

The consideration of Google's intent in this context is inappropriate. While it may have been appropriate to look at in determining *what* Google was doing, and in identifying possible procompetitive justifications, the intent behind Google's practices is irrelevant. What matters is their actual effects on consumers.

The *McWane* Case

Meanwhile, the FTC's staff recently fell prey to the lure of non-economic evidence in bringing its recent administrative collusion and exclusion case against McWane, a manufacturer of iron pipe fittings. Fortunately, the ALJ threw out a significant portion of the case on the grounds that the Complaint Counsel did not make out an economically rigorous case, noting that its evidence was "weak," "unsupported speculation" and that its "daisy chain of assumptions fails to support or justify an evidentiary inference of any unlawful agreement involving McWane."[32]

On the other hand, while the Commissioners upheld the ALJ's ruling against the Commission on the conspiracy counts,[33] a majority of the Commissioners (with Commissioner Wright dissenting) missed the full economic significance of the evidence at trial and held in favor of the Commission's Complaint Counsel on the exclusion count — largely because one of McWane's competitors "made self-serving assertions that it would have had more business but for the defendant's action and would have had lower per-unit costs if it had more business."[34]

In fact, Complaint Counsel relied entirely on business documents to make its case — and a majority of the Commission accepted its arguments. The Commission's expert report on the monopolization count was little more than an economist reciting the theoretical conditions in the economic literature for exclusive dealing to harm competition — with no evidence pointing to the actual anticompetitive outcomes necessary to properly make a case. As Commissioner Wright noted in his dissent from this portion of the holding, this lapse had significant effect,

---

[32] In the Matter of McWane, Inc., Docket No. 9351, Initial ALJ Decision, at 286, 300, 306-07 (May 8, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130509mcwanechappelldecision.pdf.

[33] *See* In the Matter of McWane Inc., Docket No. 9351, Opinion of the Commission (Feb. 6, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140206mcwaneopinion.pdf.

[34] Thom Lambert, *Commissioner Wright's McWane Dissent Illuminates the Law and Economics of Exclusive Dealing*, TRUTH ON THE MARKET (Feb. 17, 2014), http://truthonthemarket.com/2014/02/17/commissioner-wrights-mcwane-dissent-illuminates-the-law-and-economics-of-exclusive-dealing/.

essentially rewriting the well-accepted standards required to prove a violation of Section 2 of the Sherman Act:

> [N]either Complaint Counsel nor the Commission provides an analytical link between Complaint Counsel's foreclosure analysis and competitive harm… — that is, evidence consistent with Complaint Counsel's theory and Complaint Counsel and the Commission's assertion that the level of foreclosure was sufficient to cause competitive harm over the time it was in effect. Neither Complaint Counsel nor the Commission makes any attempt to reconcile the absence of actual evidence of anticompetitive effects with the high foreclosure rates they claim are at issue. Because foreclosure rates are relevant only as a proxy for better understanding competitive effects, this failure undermines the Commission's heavy reliance upon inferences drawn from foreclosure rates. By concluding that Complaint Counsel need only demonstrate that [McWane's competitor] was foreclosed from some unspecified amount of distributors as a result of the [McWane's exclusive dealing program], without linking that foreclosure to the preservation of McWane's monopoly power, the Commission in effect holds that harm to a competitor without more is sufficient to establish a violation of Section 2.[35]

As Wright points out in his dissent, if there were evidence of actual harm it would have been readily available to Complaint Counsel because the conduct at issue in the case occurred in the past. Instead, Complaint Counsel (which was authorized by the Commission to pursue the case) made an affirmative choice to forego adducing this economic evidence and to rely instead on "hot" docs rather than "cold" economics. In accepting this evidence a majority of the Commission produced an outcome unsupported by the evidence and in violation of one of the first, cardinal rules of antitrust:

> Because antitrust exists to protect competition, not competitors, an antitrust complainant cannot base a claim of monopolization on the mere fact that its business was injured by the defendant's conduct…. If antitrust is to remain a consumer-focused body of law, claims like [McWane's competitor's] should fail. Hopefully, Commissioner Wright's FTC colleagues will eventually see that point.[36]

Unfair Methods of Competition and Guidelines

As antitrust law began to shift toward the "rule of reason," the FTC began, in the 1980s, to push the boundaries of its UMC authority beyond the traditional antitrust laws in a trio of

---

[35] In the Matter of McWane Inc., Docket No. 9351, Dissenting Statement of Commissioner Joshua D. Wright at 37 (Feb. 6, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140206mcwanestatement.pdf.

[36] Lambert, *supra* note 34.

cases.[37] However, the FTC's position was roundly rejected by the courts. Advocates for a more expansive approach to antitrust law generally have continued to advocate the view that Section 5 incorporates, but expands beyond, the "antitrust laws," however.[38] Importantly, the room for such expansion exists because the FTC has never limited its discretion to interpret or enforce its UMC authority with Guidelines or other express limiting principles.

Among the agency's activities, the issuing of guidelines, policy statements, advisory letters and the like regarding its own authority are unique in that they tend to *restrain* the scope of the agency's discretion rather than expand it. Other than increased judicial oversight (or legislated jurisdictional limitations), such guidance may be the most effective procedural tool for cabining agency discretion.

Ideally, the agency's guidelines and policy statements would be constituted to accurately reflect agency practice and legal interpretations, offering insight into the agency's decision-making process, the benefits of its expertise and a clear signal of its likely future actions. Because guidelines are not binding,[39] actual enforcement (and regulatory) actions may deviate from their prescriptions. However, guidelines and other policy statements may have important effect on subsequent agency actions. For instance, they may affect a court's subsequent evaluation of an agency action, or provide potential litigants with insights needed to mount an effective judicial challenge. Should the agency act contrary to its published position, this may provide impetus for Congressional scrutiny of the agency. Moreover, deviation from its prior published statements may incur reputational harms of concern to the Commission. And importantly, to the extent that guidelines incorporate well-established economic principles, deviation from them may be readily apparent and subject to criticism from economists and economically savvy practitioners.

Despite (or because of) their imposition of constraints on discretion, some of the FTC's guidelines have been enormously successful. The Horizontal Merger Guidelines have historically "provide[d] a flexible, comprehensive, and administrable approach," while still remaining both "broadly applicable and providing certainty to businesses and practitioners."[40] Moreover, they seem, generally, to reflect actual agency practice. That said, it is telling to note

---

[37] *See* E.I. duPont de Nemours & Co. v. FTC, 729 F.2d 128 (2d Cir. 1984); Boise Cascade v. FTC, 637 F.2d 573 (9th Cir. 1980); Official Airline Guides v. FTC, 630 F.2d 920 (2d Cir. 1980).

[38] For an informative discussion on the FTC's UMC authority and Commissioner Wright's call for more guidance from a variety of perspectives, see Truth on the Market Blog Symposium on UMC (Aug. 1-2, 2013), http://truthonthemarket.com/category/umc-symposium/.

[39] DISH Network, LLC v. FCC and United States, No. 13-1182 (D.C. Cir. Jan. 22, 2014).

[40] Timothy J. Muris and Bilal Sayyed, *Three Key Principles for Revising the Horizontal Merger Guidelines*, ANTITRUST SOURCE 3-4 (April 2010), *available at* http://www.law.gmu.edu/assets/files/publications/working_papers/1256ThreeKeyPrinciples.pdf.

that the FTC and DOJ's decision to revise these guidelines in 2010 has been met with criticism. It remains to be seen how they will be embraced by the courts and what lasting effects they will have on merger review.

Unfair Methods of Competition

As in other areas, the Commission is playing with fire in its UMC cases. And here, because the FTC's authority is drawn directly from Section 5, and because there is vanishingly little in the way of judicial decisions to interpret the statute or cabin the FTC's discretion, the FTC's pursuit of Section 5 as an independent basis to bring competition claims not recognized by the antitrust laws risks upending the analytical discipline provided by economics.

Section 5 enforcement standards in the unfairness context are non-existent. Former Chairman Leibowitz and former Commissioner Rosch, in particular, have, in several places, argued for an expanded use of Section 5, both as a way around judicial limits on the scope of Sherman Act enforcement, as well as as an affirmative tool to enforce the FTC's mandate. As the Commission's statement in the *N-Data* case concluded:

> We recognize that some may criticize the Commission for broadly (but appropriately) applying our unfairness authority to stop the conduct alleged in this Complaint. But the cost of ignoring this particularly pernicious problem is too high. Using our statutory authority to its fullest extent is not only consistent with the Commission's obligations, but also essential to preserving a free and dynamic marketplace.[41]

The problem is that neither the Commission, the courts nor Congress has defined what, exactly, the "fullest extent" of the FTC's statutory authority is. And, as Commissioner Wright noted in his speech introducing his proposed UMC Policy Statement, "[i]n practice…, the scope of the Commission's Section 5 authority today is as broad or as narrow as a majority of the commissioners believes that it is."[42] The Commission's claim that it applied its authority "broadly (but appropriately)" in *N-Data* is unsupported and unsupportable. As Commissioner Ohlhausen put it in her dissent in *In re Bosch*,

> I simply do not see any meaningful limiting principles in the enforcement policy laid out in these cases. The Commission statement emphasizes the context here (i.e. standard setting); however, it is not clear why the type of conduct that is targeted here (i.e. a

---

[41] In the Matter of Negotiated Data Solutions LLC., Statement of the Commission at 3, *available at* http://www.ftc.gov/os/caselist/0510094/080122statement.pdf.

[42] Joshua Wright, *Section 5 Recast: Defining the Federal Trade Commission's Unfair Methods of Competition Authority* (Jun. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/section-5-recast-defining-federal-trade-commissions-unfair-methods-competition-authority/130619section5recast.pdf.

> breach of an allegedly implied contract term with no allegation of deception) would not be targeted by the Commission in any other context where the Commission believes consumer harm may result. If the Commission continues on the path begun in *N-Data* and extended here, we will be policing garden variety breach-of-contract and other business disputes between private parties.
>
> * * *
>
> It is important that government strive for transparency and predictability. Before invoking Section 5 to address business conduct not already covered by the antitrust laws (other than perhaps invitations to collude), the Commission should fully articulate its views about what constitutes an unfair method of competition, including the general parameters of unfair conduct and where Section 5 overlaps and does not overlap with the antitrust laws, and how the Commission will exercise its enforcement discretion under Section 5. Otherwise, the Commission runs a serious risk of failure in the courts and a possible hostile legislative reaction, both of which have accompanied previous FTC attempts to use Section 5 more expansively.
>
> This consent does nothing either to legitimize the creative, yet questionable application of Section 5 to these types of cases or to provide guidance to standard-setting participants or the business community at large as to what does and does not constitute a Section 5 violation. Rather, it raises more questions about what limits the majority of the Commission would place on its expansive use of Section 5 authority.[43]

The FTC has never explained what its "unfair methods of competition" authority covers that antitrust doesn't. Commissioner Wright recently proposed limiting principles, but FTC Chairman Edith Ramirez appears reluctant to relinquish any discretion. Wright's proposed guidance would bring not only an appropriate economic framework to bear on UMC cases — one that mimics the guidance and judicial opinions that govern in Sherman and Clayton Act cases — but would provide a constraint on unfettered agency discretion.[44]

Commissioner Wright's proposed UMC Policy Statement attempts to remedy these defects, and, in the process, explains why the Commission's previous, broad applications of the statute are not, in fact, appropriate. His draft statement, along with the policy speech in which he

---

[43] In the Matter of Robert Bosch GmbH, FTC File No. 121-0081 (Commissioner Ohlhausen, dissenting), at 3-4, *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-ohlhausen/121126boschohlhausenstatement.pdf [hereinafter "Ohlhausen Bosch Dissent"].

[44] Joshua Wright, *Proposed Policy Statement Regarding Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act* (Jun. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-joshua-d.wright/130619umcpolicystatement.pdf [hereinafter "Wright, *Proposed Policy Statement*"].

introduced it,[45] present a compelling and comprehensive vision for Section 5 UMC reform at the Commission.

At the outset of his statement Wright invokes the importance of limiting principles:

> In order for enforcement of its unfair methods of competition authority to promote consistently the Commission's mission of protecting competition, the Commission must articulate a clear framework for its application.[46]

Significantly, in addition to offering important certainty to guide business actions, Wright bases his proposed policy statement on the error cost framework:

> The Commission must formulate a standard that distinguishes between acceptable business practices and business practices that constitute an unfair method of competition in order to provide firms with adequate guidance as to what conduct may be unlawful. Articulating a clear and predictable standard for what constitutes an unfair method of competition is important because the Commission's authority to condemn unfair methods of competition allows it to break new ground and challenge conduct based upon theories not previously enshrined in Sherman Act or Clayton Act jurisprudence.

Such restraint is crucial at the FTC. Efforts by the agency's immediate past Chairman and others to expand Section 5 to challenge conduct under novel theories, devoid of economic grounding and without proof of anticompetitive harm (in cases like *Intel*,[47] *N-Data*[48] and *Google*,[49] among others) brought into stark relief the potential risks of an unfettered Section 5.

Particularly given the novelty of circumstances that might come within Section 5's ambit, the error-cost minimizing structure of Commissioner Wright's proposed statement is enormously important. As Wright and I note in a co-authored paper, *Innovation and the Limits of Antitrust*:

> Both product and business innovations involve novel practices, and such practices generally result in monopoly explanations from the economics profession followed by hostility from the courts (though sometimes in reverse order) and then a subsequent,

---

[45] *See* Wright, *Section 5 Recast*, *supra* note 42.

[46] Wright, *Proposed Policy Statement*, *supra* note 44, at 2.

[47] In the Matter of Intel Corp., Docket No. 9341, http://www.ftc.gov/enforcement/cases-proceedings/061-0247/intel-corporation-matter.

[48] In the Matter of Negotiated Data Solutions LLC., FTC File No. 051 0094, http://www.ftc.gov/enforcement/cases-proceedings/051-0094/negotiated-data-solutions-llc-matter.

[49] In the Matter of Motorola Mobility LLC and Google Inc., FTC File No. 1210120, http://www.ftc.gov/enforcement/cases-proceedings/1210120/motorola-mobility-llc-google-inc-matter.

> more nuanced economic understanding of the business practice usually recognizing its procompetitive virtues.[50]

And as Wright's statement notes,

> This is particularly true if business conduct is novel or takes place within an emerging or rapidly changing industry, and thus where there is little empirical evidence about the conduct's potential competitive effects.[51]

The high cost and substantial risk of false positives arising from unbounded Section 5 authority counsel strongly in favor of Wright's statement restricting Section 5 to minimize these error costs.

In important ways the real work in Wright's statement is done by the limitation on UMC enforcement in cases where the complained-of practice produces cognizable efficiencies. In his framing it is not a balancing test or a rule of reason. It is a safe harbor for cases where conduct is efficient, regardless of its effect on competition otherwise:

> The Commission therefore creates a clear safe harbor that provides firms with certainty that their conduct can be challenged as an unfair method of competition only in the absence of efficiencies.[52]

Wright's Proposed UMC Statement is the most important and ambitious effort to date to incorporate the error cost framework into FTC antitrust enforcement policy. This aspect of the statement takes seriously the harm that can arise from the agency's discretion, uncertainty over competitive effects (especially in "likely to cause" cases) and the imbalance of power and costs inherent in the FTC's Part III adjudication to tip the scale back toward avoidance of erroneous over-enforcement.

In essence, by removing the threat of Section 5 enforcement where efficiencies are cognizable, Wright's statement avoids the risk of Type I error, prioritizing the possible realization of efficiencies over possible anticompetitive harm with a bright line rule that avoids attempting to balance the one against the other:

> The Commission employs an efficiencies screen to establish a test with clear and predictable results that prevents arbitrary enforcement of the agency's unfair methods of competition authority, to focus the agency's resources on conduct most likely to

---

[50] Manne & Wright, *Innovation & Limits*, *supra* note 1, at 165.

[51] Wright, *Proposed Policy Statement*, *supra* note 44, at 11.

[52] *Id.* at 10.

> harm consumers, and to avoid deterring consumer welfare-enhancing business practices.[53]

Fundamentally, as Commissioner Wright explained in his speech,

> Anticompetitive conduct that lacks cognizable efficiencies is the most likely to harm consumers because it is without any redeeming consumer benefits. The efficiency screen also works to ensure that welfare-enhancing conduct is not inadvertently deterred.... The Supreme Court has long recognized that erroneous condemnation of procompetitive conduct significantly reduces consumer welfare by deterring investment in efficiency-enhancing business practices. To avoid deterring consumer welfare-enhancing conduct, my proposed Policy Statement limits the use of Section 5 to conduct that lacks cognizable efficiencies.[54]

Wright's statement encapsulates the sort of economic principles — both in substance and in regulatory form — that would bring the sound economic grounding of antitrust law and economics to Section 5, benefiting consumers as well as commerce generally:

> This Policy Statement benefits both consumers and the business community by relying on modern economics and antitrust jurisprudence to strengthen the agency's ability to target anticompetitive conduct and provide clear guidance about the contours of the Commission's Section 5 authority.[55]

Importantly, this is as much about preserving the FTC itself as it is about good economics:

> In undertaking this task, I think it is important to recall why the Commission's use of Section 5 has failed to date. In my view, this failure is principally because the Commission has sought to do too much with Section 5, and in so doing, called into serious question whether it has any limits whatsoever. In order to save Section 5, and to fulfill the vision Congress had for this important statute, the Commission must recast its unfair methods of competition authority with an eye toward regulatory humility in order to effectively target plainly anticompetitive conduct..... I believe that doing anything less would betray our obligation as responsible stewards of the Commission and its competition mission, and may ultimately result in the Commission having its Section 5 authority defined for it by the courts, or worse, having that authority completely revoked by Congress.[56]

---

[53] *Id.* at 9.

[54] *Id.* at 10.

[55] *Id.* at 2.

[56] Wright, *Section 5 Recast*, *supra* note 42, at 15.

This means circumscribing the FTC's Section 5 authority to limit enforcement to cases where the Commission shows both actual harm to competition and the absence of cognizable efficiencies.

Commissioner Wright's statement does not represent a restriction of antitrust enforcement authority unless you take as your starting point the agency's recent largely unsupported and expansive interpretation of Section 5—a version of Section 5 that arguably was never intended to exist. Wright's statement is, rather, a bulwark against unprincipled regulatory expansion: a sensible grounding of a statute with a checkered past and a penchant for mischief.

Moreover, Wright's statement doesn't mean that the FTC can't bring cases in which the anticompetitive harm outweighs the efficiency benefits. As always, those cases can be, should be and are brought under the traditional antitrust laws.

Former Chairman Leibowitz and former Commissioner Rosch, in defending the use and expansion of Section 5, argued in *Intel* that it was necessary to circumvent judicial limitations on the enforcement of Section 2 aimed only at *private* plaintiffs.[57] According to Leibowitz, the Court's economically rigorous, error-cost jurisprudence in cases like *linkLine*,[58] *Trinko*,[59] *Leegin*,[60] *Twombly*,[61] and *Brook Group*[62] were aimed at private plaintiffs, not agency actions:

> But I also believe that the result, at least in the aggregate, is that some anticompetitive behavior is not being stopped—in part because the FTC and DOJ are saddled with court-based restrictions that are designed to circumscribe private litigation. Simply put, consumers can still suffer plenty of harm for reasons not encompassed by the Sherman Act as it is currently enforced in the federal courts.[63]

---

[57] Statement of Chairman Leibowitz and Commissioner Rosch, In the Matter of Intel Corporation, Docket No. 9341, http://www.ftc.gov/sites/default/files/documents/cases/091216intelchairstatement.pdf.

[58] Pacific Bell Telephone Co. v. linkLine Communications, Inc., 555 U.S. 438 (2009).

[59] Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398 (2004).

[60] Leegin Creative Leather Products, Inc. v. PSKS, Inc. 127 S. Ct. 2705 (2007).

[61] Bell Atlantic Corp. v. Twombly, 127 S. Ct. 1955 (2007).

[62] Brooke Group Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209 (1993).

[63] Jon Leibowitz, *"Tales from the Crypt" Episodes '08 and '09: The Return of Section 5 ("Unfair Methods of Competition in Commerce are Hereby Declared Unlawful")*, remarks at Section 5 Workshop (Oct. 17, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/tales-crypt.episodes-08-and-09-return-section-5-unfair-methods-competition-commerce-are-hereby-declared-unlawful/081017section5.pdf.

The claim is meritless.[64] But it helps to make clear what the problem with current Section 5 standards are: There are no standards, only post-hoc rationalizations to justify pursuing Section 2 cases without the cumbersome baggage of its jurisprudential limits.

The recent Supreme Court cases mentioned above are only the most recent examples of a decades-long jurisprudential trend incorporating modern economic thinking into antitrust law and recognizing the error-cost tradeoff.[65] These cases have served to remove certain conduct (at least without appropriate evidence and analysis) from the reach of Section 2 in a measured, accretive fashion over the last 40 years or so. They have by no means made antitrust irrelevant, and the agencies and private plaintiffs alike bring and win cases all the time—and this doesn't even measure the conduct that is deterred by the threat of enforcement.

The limits on Section 5 suggested by Commissioner Wright's statement are marginal limits on the scope of antitrust *beyond* the Sherman Act, Clayton Act and other statutes and are consistent with the generally accepted standards of Section 5.

And with Chairman Ramirez' recent speech at the 2014 George Mason Law Review Symposium on Antitrust Law, even she has essentially endorsed a "rule of reason" approach to Section 5 that requires a showing of harm to competition:

> Our most recent Section 5 cases show that the Commission will condemn conduct only where, as with invitations to collude, the likely competitive harm outweighs the cognizable efficiencies. This is the same standard we apply everyday in our investigations.[66]

While perhaps this admission doesn't go far enough, now all four currently sitting Commissioners have at least partially endorsed the idea of enumerated standards for Section 5 built on a fundamentally "rule of reason" approach. There is hope.

---

[64] *See, e.g.*, Geoffrey Manne, *The Case Against the Section 5 Case Against Intel Redux*, TRUTH ON THE MARKET (Jan. 8, 2010), http://truthonthemarket.com/2010/01/08/the-case-against-the-section-5-case-against-intel-redux-cross-posted/.

[65] *See* Leah Brannon & Douglas H. Ginsburg, *Antitrust Decisions of the U.S. Supreme Court 1967 to 2007*, 3 COMPETITION POL'Y INT'L 1 (2007), *available at* https://www.competitionpolicyinternational.com/antitrust-decisions-of-the-us-supreme-court-1967-to-2007.

[66] Edith Ramirez, Keynote, 17th Annual George Mason Law Review Symposium on Antitrust Law: "The FTC: 100 Years of Antitrust and Competition Policy" (2014), *available at* http://vimeo.com/86788312. *See also* Erica Teichert, *FTC Commissioners Spar Over Section 5 Guidance Boundaries*, LAW360 (Feb. 13, 2014), http://www.law360.com/articles/509894/ftc-commissioners-spar-over-section-5-guidance-boundaries.

Patents

Perhaps nothing the FTC does more directly implicates technology and innovation than its treatment of intellectual property. Writing about "Antitrust in the New Economy," Judge Posner noted that the "principal output of these industries… is intellectual property."[67] But as far as antitrust economics has progressed generally, it still lacks a solid understanding of the relationship among investment in R&D, market structure, price, quality, speed of innovation and welfare effects.[68] The risk of Type I error is thus particularly high, and its potential cost higher still.[69]

Nonetheless, basic economics suggests that, in unknown degrees, the production, distribution and enforcement of intellectual property will lead to standardization (coordination among competitors), the need for interoperability (and thus a greater opportunity for anticompetitive foreclosure), economies of scale (high levels of concentration), and the presence of network effects, all of which may contribute to an increased likelihood of monopolization.[70] At the same time, many question the validity of many patents and the reliability of the patent approval process, and note the potential for "greenmail." These critics have encouraged the FTC to use its UMC authority against companies asserting legally questionable or standard-essential patents (SEPs) in certain contexts.

Against this backdrop, the FTC has in recent years stepped up its enforcement around patents. Recent (and controversial) Section 5 cases against Intel,[71] Rambus,[72] Google[73] and Bosch,[74] for example, have turned on issues surrounding those firms' enforcement of SEPs. The Commission is currently conducting a 6(b) investigation into patent assertion entities, and the FTC has pursued a vigorous and lengthy war on pharmaceutical industry reverse payment settlements.

---

[67] Richard A. Posner, *Antitrust in the New Economy*, 68 ANTITRUST L.J. 925, 927 (2001).

[68] One important, recent effort to overcome this lack is Daniel F. Spulber, *How Do Competitive Pressures Affect Incentives to Innovate when there is a Market for Inventions?*, 121 J. POL. ECON. 1007 (2013).

[69] Manne & Wright, *Innovation and Limits*, *supra* note 1, at 170.

[70] *Id.* at 171.

[71] In the Matter of Intel Corp., Docket No. 9341, http://www.ftc.gov/enforcement/cases-proceedings/061-0247/intel-corporation-matter.

[72] In the Matter of Rambus Inc., Docket No. 9302, http://www.ftc.gov/enforcement/cases-proceedings/110017/rambus-inc-matter.

[73] In the Matter of Motorola Mobility LLC and Google Inc., FTC File No. 1210120, http://www.ftc.gov/enforcement/cases-proceedings/1210120/motorola-mobility-llc-google-inc-matter.

[74] In the Matter of Robert Bosch GmbH, FTC File No. 121-0081, http://www.ftc.gov/enforcement/cases-proceedings/1210081/bosch-robert-bosch-gmbh.

The question of the appropriate application of UMC to patent issues, particularly to police the enforcement of SEPs through the threat of injunctions and the breach of FRAND requirements by certain patent holders, is a controversial one. But here as elsewhere the core of the controversy may rest in the appropriate exercise of discretion generally rather than as applied to patents in particular. As Commissioner Ohlhausen wrote in dissenting from the Commission's action in Bosch:

> I simply do not see any meaningful limiting principles in the enforcement policy laid out in these cases. The Commission statement emphasizes the context here (i.e. standard setting); however, it is not clear why the type of conduct that is targeted here (i.e. a breach of an allegedly implied contract term with no allegation of deception) would not be targeted by the Commission in any other context where the Commission believes consumer harm may result.[75]

Applying Section 5 to FRAND-encumbered SEPs, as I have discussed at length elsewhere, is problematic.[76] As Kobayashi and Wright note in discussing the *N-Data* case,

> [T]he truth is that there was little chance the FTC could have prevailed under the more rigorous Section 2 standard that anchors the liability rule to a demanding standard requiring proof of both exclusionary conduct and competitive harm. One must either accept the proposition that the FTC sought Section 5 liability precisely because there was no evidence of consumer harm or that the FTC believed there was evidence of consumer harm but elected to file the Complaint based only upon the Section 5 theory to encourage an expansive application of that Section, a position several Commissioners joining the Majority Statement have taken in recent years. Neither of these interpretations offers much evidence that N-Data is sound as a matter of prosecutorial discretion or antitrust policy.[77]

None of the FTC's SEP cases has offered anything approaching proof of consumer harm, and this is where any sensible, economically grounded limiting principles must begin. Moreover, even if they did adduce evidence of harm, the often-ignored problem of reverse hold-up raises precisely the concern about over-enforcement that the "no efficiencies" prong in Commissioner Wright's UMC Policy Statement (discussed above) is meant to address. Hold-up

---

[75] Ohlhausen, Bosch Dissent, *supra* note 43, at 3.

[76] *See* International Center for Law & Economics Comment Regarding the Proposed Order, In the Matter of Motorola Mobility LLC and Google, Inc., File No.121-0120, *available at* http://laweconcenter.org/images/articles/icle_comment_google_order.pdf.

[77] Bruce Kobayashi & Joshua Wright, *Federalism, Substantive Preemption, And Limits On Antitrust: An Application To Patent Holdup*, 5 J. COMPETITION L. & ECON. 469, 495 (2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1143602.

may raise consumer prices (although the FTC has not presented evidence of this), but reverse hold-up may do as much or more damage.

And, as it happens, true hold-ups are exceedingly rare; even in the literature there are few examples of actual hold-ups (or patent thickets) impeding innovation. Thus, while competition law might offer a potential benefit from preventing those few cases, it is unlikely that such benefit would exceed the serious effects on innovation, standardization and patent licensing that an antitrust-based constraint on patent rights would engender.

The use of injunctions to enforce SEPs strengthens property rights and, in turn, increases innovation investment, the willingness to license generally and the willingness to enter into FRAND commitments in particular – all to the likely benefit of consumer welfare. If the FTC interprets its UMC authority in a way that constrains the ability of patent holders to effectively police their patent rights, then less innovation would be expected–to the detriment of consumers as well as businesses. An unfettered UMC authority will systematically curtail these benefits, quite possibly with only trivial countervailing positive effects.

And, as I have pointed out before, these costs are real.[78] Innovative technology companies are responding to the current SEP enforcement environment exactly as we would expect them to: by avoiding the otherwise-consumer-welfare-enhancing standardization process entirely:

> Because of the current atmosphere, Lukander said, Nokia has stepped back from the standardisation process, electing either not to join certain standard-setting organisations (SSOs) or not to contribute certain technologies to these organisations.[79]

Section 5 is a particularly problematic piece of this, and sensible limits would go a long way toward mitigating the problem—without removing enforcement authority in the face of real competitive harm, which remains available under the Sherman Act.

Meanwhile, as noted above, whatever the propriety of the application of Section 5 to these issues, there remains important questions regarding the appropriateness of competition-policy enforcement in this realm at all.

In the first place, the upshot of the FTC's range of actions against patents is, in varying degrees, to move the property rule of patents (enforceable by injunction) more towards a

---

[78] *See* Geoffrey Manne, *The Final Order in the FTC's Google SEP Case and the Continuing Danger to Standard-Setting*, TRUTH ON THE MARKET (Jul. 31, 2013), http://truthonthemarket.com/2013/07/31/the-final-order-in-the-ftcs-google-standard-essential-patents-case-and-the-continuing-danger-to-standard-setting/.

[79] Katy Oglethorpe, *Nokia counsel: major companies "willfully infringe" FRAND,* GLOBAL COMPETITION REVIEW (Jun. 17, 2013), http://globalcompetitionreview.com/news/article/33655/nokia-counsel-major-companies-wilfully-infringe-frand/.

liability rule (enforceable by royalty payments). While the aim is the weakening of patent rights under the theory that doing so will promote innovation and welfare, this assumption, although widely repeated, is by no means established.[80]

Among other things, to the extent that the FTC's SEP actions are motivated by concerns about hold-up problems arising from refusals to license essential IP, it is not evident that the FTC is sufficiently sensitive to the analogous "holdout" problem of potential licensees taking advantage of lax enforcement in order to infringe — an effect that would manifestly lower, not raise, incentives for innovation.[81]

Fundamentally, there remain important questions regarding the benefits for consumer welfare from antitrust interference in IP markets in general. Neither the FTC, nor the academy in general, has resolved these questions, but nevertheless their conduct suggests they have. But as Dan Spulber discusses in a recent, important article:

> [A]ntitrust policy and IP protections are complements in promoting innovation. With effective IP protections, policies that favor competition including antitrust and deregulation can help to speed innovation. But, absent effective IP protections, antitrust policy may actually be harmful because it would diminish incentives to innovate. Applying antitrust policy to weaken appropriability of IP thus would be counter productive. There is some disagreement among economists, legal scholars, and the courts on whether antitrust and IP policies should be viewed as being consistent or in conflict. The present analysis suggests instead that antitrust policy and IP protections should be consistent in encouraging innovation and competition.[82]

Consumer Protection

Consumer protection law, unlike antitrust law, has increasingly been shaped primarily by the FTC's discretion, not evolution through judicial review or dialogue with economic scholarship. In the last decade, the FTC has increasingly been using its unfairness authority to address cutting-edge issues. It has even begun pushing the legal boundaries of its authority over deception by extending it beyond traditional advertising claims to online FAQs and the like.

At the heart of the discretionary model is the FTC's ability to operate without any real constraints. The Commission hasn't developed a predictable set of legal doctrines because that's what courts do — and the FTC has managed to strong-arm dozens of companies into

---

[80] *See, e.g.*, F. Scott Kieff, *IP Transactions: On the Theory & Practice of Commercializing Innovation*, 42 HOUSTON L. REV. 727 (2005).

[81] *See, e.g.*, Manne, *Continuing Danger*, *supra* note 78.

[82] Spulber, *Competitive Pressures*, *supra* note 68, at 1009.

settling out of court. What the FTC calls its "common law of consent decrees" is really just a series of unadjudicated assertions. That approach is just as top-down and technocratic as the FCC's regulatory model, but with little due process and none of the constraints of detailed authorizing legislation.

The FTC might be right in any particular case, but overall, what evolves isn't "law." It's merely a list of assertions as to what the Commission thinks companies should and shouldn't do. Unfortunately current and recent FTC leadership has shown little interest in limiting the agency's discretion. In a similar context Commissioner Ohlhausen has pointedly noted:

> The guidance in the Policy Statement will be replaced by this view: "[T]he Commission withdraws the Policy Statement and will rely instead upon existing law, which provides sufficient guidance on the use of monetary equitable remedies." This position could be used to justify a decision to refrain from issuing any guidance whatsoever about how this agency will interpret and exercise its statutory authority on any issue.[83]

UDAP: The *Apple* Case

The FTC's recent complaint and consent agreement with Apple highlights these issues, and, again, Commissioner Wright's scathing dissent ably identifies where and how the agency deviated from sensible economic reasoning.

The Commission's unfairness authority under Section 5 of the FTC Act is circumscribed by subsection (n), which itself tracks language issued by the FTC in its 1980 Unfairness Policy Statement. Section 45(n) actually incorporates sensible economic limiting principles:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair **unless the act or practice causes or is likely to cause substantial injury to consumers** which is **not reasonably avoidable by consumers themselves** and **not outweighed by countervailing benefits to consumers or to competition**.[84] [Emphasis added].

The core requirements (that injury be substantial, that it not be reasonably avoidable by consumers and that it not be outweighed by countervailing benefits) serve to enshrine an error cost approach to unfairness questions, limiting both the likelihood and harm of erroneous over-enforcement.

---

[83] Statement of Commissioner Maureen K. Ohlhausen Dissenting from the Commission's Decision to Withdraw its Policy Statement on Monetary Equitable Remedies in Competition Cases (Jul. 31, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/120731ohlhausenstatement.pdf.

[84] 15 U.S.C. §45, http://www.law.cornell.edu/uscode/text/15/45.

One of the key reasons for performing a cost-benefit analysis as required by the FTC's Policy Statement (and subsequently codified in Section 5) is to ensure that government action does more good than harm. As Commissioner Wright succinctly puts it in his *Apple* dissent:

> To justify a finding of unfairness, the Commission must demonstrate the allegedly unlawful conduct results in net consumer injury.[85]

That such a balancing was absent from the majority's decision in *Apple* reflects not only dereliction of a legal obligation by the Commission, but also the subversion of sensible economic analysis. As Wright notes:

> The Commission, under the rubric of "unfair acts and practices," substitutes its own judgment for a private firm's decisions as to how to design its product to satisfy as many users as possible, and requires a company to revamp an otherwise indisputably legitimate business practice. Given the apparent benefits to some consumers and to competition from Apple's allegedly unfair practices, I believe the Commission should have conducted a much more robust analysis to determine whether the injury to this small group of consumers justifies the finding of unfairness and the imposition of a remedy.[86]

Undertaking an appropriate cost-benefit analysis — as the Commission's own Policy Statement requires — would have yielded a different result given available facts:

> In particular, although Apple's allegedly unfair act or practice has harmed some consumers, I do not believe the Commission has demonstrated the injury is substantial. More importantly, any injury to consumers flowing from Apple's choice of disclosure and billing practices is outweighed considerably by the benefits to competition and to consumers that flow from the same practice.[87]

---

[85] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Apple, Inc., FTC File No. 1123108, at 14 (Jan. 15, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf [hereinafter "Wright *Apple* Dissent"].

[86] *Id.* at 1-2. While Commissioner Wright's dissent is remarkable for demanding a new level of analytical rigor in a consumer protection case, it is neither novel nor aberrant in the larger context of the FTC's work. In fact, the kind of law and economics Wright proposes should be applied in weighing unfairness has long been applied in antitrust cases. And the substantive position that analysis leads him to dovetails with the prevailing *per se* rule in antitrust law that there is no liability for "predatory" innovation or product design. *See, e.g.*, Allied Orthopedic v. Tyco, 592 F.3d 991 (9th Cir. 2010). Even the standard in *Microsoft*, which the court in *Tyco* rejected, required a balancing of costs and benefits and, ultimately, proof by the plaintiff that the harm to consumers outweighed the defendant's justifications for its design decisions. *Cf.* U.S. v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001).

[87] Wright *Apple* Dissent, *supra* note 85, at 2.

What's particularly notable about the *Apple* case—and presumably will be in future technology enforcement actions predicated on unfairness—is the unique relevance of the attributes of the conduct at issue to its product. Unlike past, allegedly similar cases, Apple's conduct was not aimed at deceiving consumers, and nor was it incidental to its product offering. Instead, as Wright notes:

> [R]ather than an unscrupulous or questionable practice, the nature of Apple's disclosures on its platform is an important attribute of Apple's platform that affects the demand for and consumer benefits derived from Apple devices and services. Disclosures made on the screen while consumers interact with mobile devices are a fundamental part of the user experience for products like mobile computing devices. It is well known that Apple invests considerable resources in its product design and functionality. In streamlining disclosures on its platform and in its choice to integrate the fifteen-minute window into Apple users' experience on the platform, Apple has apparently determined that most consumers do not want to experience excessive disclosures or to be inconvenienced by having to enter their passwords every time they make a purchase.[88]

But by challenging the practice, particularly without the balancing of harms required by Section 5, the FTC majority substituted its own judgment not about some manifestly despicable conduct but about the very design of Apple's products. This is the sort of area where regulatory humility is more — not less — important:

> With complex technology products such as computing platforms, firms generally find and address numerous problems as experience is gained with the product. Virtually all software evolves this way, for example. This tradeoff— between time spent perfecting a platform up front versus solving problems as they arise—is also relevant for evaluating unfairness.
>
> * * *
>
> Nonetheless, the Commission effectively rejects an analysis of tradeoffs between the benefits of additional guidance and potential harm to some consumers or to competition from mandating guidance by assuming that "the burden, if any, to users who have never had unauthorized charges for in-app purchases, or to Apple, from the provision of this additional information is de minimis" and that any mandated disclosure would not "detract in any material way from a streamlined and seamless user experience." I respectfully disagree. These assumptions adopt too cramped a view of

[88] *Id.* at 4.

> consumer benefits under the Unfairness Statement and, without more rigorous analysis to justify their application, are insufficient to establish the Commission's burden.[89]

Again, regulatory self-restraint is even more needed with complex, technologically advanced products of the sort the Commission is increasingly asked to assess, and the FTC's Unfairness Statement itself requires the Commission to "consider the impact of contemplated remedies or changes in the incentives to innovate new product features upon consumers and competition."[90] In failing to observe such limits in *Apple*, the FTC set a dangerous precedent that, given the agency's enormous regulatory scope, could cause significant harm to consumers. As Wright concludes:

> Establishing that it is "unfair" unless a firm anticipates and fixes such problems in advance – precisely what the Commission's complaint and consent order establishes today – is likely to impose significant costs in the context of complicated products with countless product attributes. These costs will be passed on to consumers and threaten consumer harm that is likely to dwarf the magnitude of consumer injury contemplated by the complaint.[91]

UDAP: The *Amazon.com* Case

More recently the FTC has doubled down on its flawed approach to unfairness with a similar action against Amazon.com.[92] Amazon, however, has decided to challenge the FTC's enforcement and has refused to settle with the Commission:

> In a letter to the FTC… Amazon said it was prepared to "defend our approach in court," rather than agree to fines and additional record keeping and disclosure requirements over the next 20 years, according to documents reviewed by The Wall Street Journal.[93]

The FTC's case against Amazon,[94] while bearing out my prediction that we would see more cases like *Apple* where the conduct in question bears on a core feature of the accused company's product offerings, is arguably even more egregious than the case against Apple.

---

[89] *Id.* at 11-12, 13.

[90] *Id.* at 15 (*citing* Unfairness Statement at 1073-74).

[91] *Id.* at 16.

[92] FTC v. Amazon.com, Inc., Case No. 2:14-cv-01038 (W.D. Wash. 2014).

[93] Greg Bensinger, "Amazon Resisting FTC on Policy Change for In-App Purchases," WALL STREET J. (Jul. 2, 2014), http://online.wsj.com/articles/amazon-resisting-ftc-on-in-app-purchases-by-children-1404317383.

[94] The FTC's Complaint is available at http://www.ftc.gov/system/files/documents/cases/140710amazoncmpt1.pdf [hereinafter "Amazon Complaint"].

Amazon has built its entire business around (indeed, event patented) the "1-click" concept (which consumers seem to value considerably above $0) and implemented a host of notification and security processes hewing as much as possible to that design choice, but nevertheless taking account of the sorts of issues raised by in-app purchases. Moreover, and perhaps most significantly, it has implemented a comprehensive parental control regime (including the ability to turn off all in-app purchases) called Kindle Free Time that arguably goes well beyond anything the FTC required in its *Apple* consent order.[95]

In *Amazon*, the FTC reinforces its approach to unfairness that effectively converts the balancing of harms and benefits required under Section 5 of the FTC Act to a *per se* rule that deems certain practices to be unfair *regardless of countervailing benefits*. Similarly, it is attempting to extend the informed consent standard it created in *Apple* that essentially maintains that only specific, identified practices (essentially, distinct notification at the time of purchase or opening of purchase window, requiring entry of a password to proceed) are permissible under the Act.

Unfortunately, the FTC's approach significantly intrudes upon the editorial discretion of companies such as Amazon to make product design decisions and supersedes their judgment about which user interface designs will, on balance, benefit consumers. The FTC Act does not empower the Commission to disregard the consumer benefits of practices that simply fail to mimic the FTC's preconceived design preferences. While that sort of approach might be defensible in the face of manifestly harmful practices like cramming, it is wholly inappropriate in the context of app stores like Amazon's that spend considerable resources to design every aspect of their interaction with consumers—and that seek to attract, not to defraud, consumers.

By challenging the action rather than settling, Amazon will enable the courts to confront the FTC's approach. Under Section 5 of the FTC Act, the Commission will have to prevail on all three elements required to prove unfairness under Section 5: that there is substantial injury, that consumers can't reasonably avoid the injury and that any countervailing benefits don't outweigh the injury. Consistent with its complaint and consent order in *Apple*, the *Amazon* complaint focuses almost entirely on only the first of these. While that may have been enough to induce Apple to settle out of court, the FTC will actually have to make out a case on reasonable avoidance and countervailing benefits at trial. It is not at all clear that the agency will be able to do so on the facts alleged:

> Amazon offers thousands of apps through its mobile app store, including games that children are likely to play. In many instances, after installation, children can obtain

[95] Kindle Free Time App, http://www.amazon.com/gp/feature.html?docId=1000863021.

> virtual items within a game, many of which cost real money. Amazon bills charges for items that cost money within the app—"in-app charges"—to the parent. Amazon began billing for in-app charges in November 2011, well after media reports about children incurring unauthorized charges in similar apps from other mobile app stores. Amazon nonetheless often has failed to obtain parents' or other account holders' informed consent to in-app charges incurred by children. Just weeks after Amazon began billing for in-app charges, consumer complaints about unauthorized charges by children on Amazon's mobile devices reached levels an Amazon Appstore manager described as "near house on fire[.]" In total, parents and other Amazon account holders have suffered significant monetary injury, with thousands of consumers complaining about unauthorized in-app charges by their children, and many consumers reporting up to hundreds of dollars in such charges.[96]

On reasonable avoidance, over and above Amazon's general procedures that limit unwanted in-app purchases, the FTC may have a tough time showing that Amazon's Kindle Free Time doesn't provide parents with more than enough ability to reasonably avoid injury (the third prong of unfairness). In fact, the complaint doesn't mention Free Time at all.

But this is a glaring lapse that highlights the myopic nature of the FTC's approach. Among other things, the complaint asserts that Amazon knew about issues with in-app purchasing by December of 2011 and claims that "[n]ot until June 2014 did Amazon change its in-app charge framework to obtain account holders' informed consent for in-app charges on its newer mobile devices."[97] But Kindle Free Time was introduced in September of 2012. While four FTC Commissioners may believe that Free Time is not a sufficient response to the alleged problem, it is nevertheless a readily available, free and effective (read: reasonable) mechanism for parents to avoid the alleged harms. It may not be what the design mavens at the FTC would have chosen to do, but it seems certain that avoiding unauthorized in-app purchases by children was part of what motivated Amazon's decision to create and offer Free Time.

On countervailing benefits, as Commissioner Wright discussed in detail in his *Apple* Dissent, the Commission seems to think that it can simply assert that there are no countervailing benefits to Amazon's design choices around in-app purchases. Here the complaint doesn't mention 1-Click at all, which is core to Amazon's user interface design and surely essential to properly evaluating the balance of harms and benefits required by the FTC Act.[98]

Even if it can show that Amazon's in-app purchase practices caused harm, the Commission will still have to demonstrate that Amazon's conscious efforts to minimize the steps required to

---

[96] Amazon Complaint, *supra* note 94, at ¶ 8.

[97] *Id.* at ¶ 27.

[98] 15. U.S.C. § 45(n)

make purchases doesn't benefit consumers on balance. In *Apple*, the FTC majority essentially (and improperly) valued these sorts of user-interface benefits at zero. It implicitly does so again here, but a court is likely to require more than such an assertion.

The FTC's approach in the *Apple* consent order effectively maintains that the agency can disregard reasonable avoidance and countervailing benefits in contravention of the statute. By following the same approach here in actual litigation, the FTC may well meet resistance from the courts, which have not yet so cavalierly dispensed with the statute's requirements.

UDAP: Data Security Cases

Through a string of more than 50 UDAP enforcement actions over the last decade, the FTC has policed how American companies protect user data. Initially, the Commission used this standard only in deception cases, reading in an implied promise of reasonableness into data security promises and holding companies responsible if actual practice was found to be unreasonable. Since 2005, however, the FTC has expanded the reasonableness approach to cases in which the company made no security promise, essentially collapsing UAP's substantial injury/countervailing benefit/reasonably avoidable elements into "reasonableness," which in turn has largely, if not explicitly, been defined by the data security standards (the "Safeguards Rule") promulgated through APA rulemaking for financial institutions under Gramm-Leach-Bliley.[99]

In principle, it makes sense treat some forms of inadequate data security as an unfair trade practice, regardless of whether the company made any promise about security. But recent experience suggests the FTC is moving toward *ex post* strict liability and away from judging the reasonableness of security precautions *ex ante* on sensible economic grounds, and making that assessment without first developing or explaining the elements of unfairness in a rigorous way. While companies, such as Wyndham, and many commentators have argued for the need for greater guidance,[100] it is not clear what shape that guidance should take.

Although some have argued that the agency's data security complaints, consent orders, speeches and Congressional testimony collectively provide sufficient guidance, the lack of more formal guidelines is notable.[101] Moreover, this set of guiding materials is notably lacking

---

[99] 16 C.F.R. § 314.

[100] *See* Amici Curiae Brief of TechFreedom, International Center for Law and Economics & Consumer Protection Scholars, FTC v. Wyndham Worldwide Corp., No. 2:13-cv-01887 (D.N.J. Jun. 17, 2013), available at http://docs.techfreedom.org/Wyndham_Amici_Brief.pdf; Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673 (2013).

[101] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014), *available at* http://columbialawreview.org/wp-content/uploads/2014/04/Solove-Hartzog.pdf. Some have

any direct discussion of the reasons data security investigations are closed (and none are likely to appear in the near future given a relatively new, informal policy strongly disfavoring such explanations).[102]

To the extent that the FTC's approach has, in fact, become a "strict liability" rule, presuming that any loss of data is *per se* proof that a company's data security practices were unreasonable, there is no evidence that the inherent trade-offs this entails between increased administrability and economic rigor, or between preventing consumer injury and imposing costs on businesses that are ultimately born by consumers, is actually desirable. Again, *how* the FTC weighs those trade-offs may be as important as the substantive conclusion of that process.

In practice, the FTC brings data security cases (under both Deception and Unfairness) based on the alleged unreasonableness of a respondent's security practices without addressing the actual Section 5 elements (materiality, substantial injury, etc.) and without connecting them to reasonableness. As Commissioner Wright discussed in his *Apple* dissent, the FTC's failure to apply Section 45(n)'s doctrinal limitations to the particular facts of a case is cause for concern, particularly in the rapidly innovating world of data security.

A recent analysis of the FTC's data security complaints shows them to be:

- considerably shorter (usually about 3 pages) than complaints in private causes of action;
- often lacking in detail about causation;
- lacking any citation to, or application of, precedent;
- obfuscating who was injured and whether injures have been mitigated;
- failing to assert any facts on reasonable avoidance, countervailing benefits, or materiality; and

---

further argued, in fact, that that the threat of action through speeches, reports and the like is preferable to more concrete statements or guidelines because they are even more flexible. *See, e.g.*, Tim Wu, *Agency Threats*, 60 DUKE L.J. 1841 (2011), *available at* http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1506&context=dlj.

[102] The FTC has issued very few closing letters on data security issues. None of them is particularly helpful. *See* FTC FOIA Request Response <on file with author>. Some of the letters are completely devoid of useful information. *See, e.g.*, Michaels Closing Letter (Jul. 26, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/closing_letters/michaels-stores-inc./120706michaelsstorescltr.pdf. To the best of our knowledge, this was the only "closing letter" regarding data security since 2009. That letter provides no details on the nature of the investigation or the reasons why it was closed. At the same time, some of the letters do, if briefly, lay out the FTC's basic reasoning, providing somewhat more helpful guidance. *See, e.g.,* Dollar Tree Letter Closing Letter (Jun. 5, 2007), *available at* http://www.ftc.gov/sites/default/files/documents/closing_letters/dollar-tree-stores-inc./070605doltree.pdf.

- asserting formulaic and conclusory causes of action which would not likely survive a *Twombly* motion to dismiss.[103]

Furthermore, failing to apply Section 45(n)'s three prongs in any meaningful way (let alone a rigorous manner) discounts the need for experimentation by companies that may become caught in the FTC's *per se* trap. It deters self-correction and consumer self-help and fails to weigh the costs and benefits of particular data security practices with reference to other characteristics (like company size, industry, threat, etc.).

At the same time, greater *ex ante* certainty (say, in the form of data security principles or a formal rulemaking) could end up sacrificing too much flexibility, possibly imposing even greater costs (of a different sort) on businesses and consumers than the current regime. Care must be taken in drafting any sort of guidance to ensure that it doesn't enshrine a particular data security regime (much as the FTC's current reliance on the Safeguards Rule has essentially done). But such guidance could, among other things:

Define the appropriate boundaries of substantial injury. Current FTC cases often rely on losses borne by companies (fraudulent charges reimbursed to consumers), rather than by consumers directly. In doing so, the FTC may in fact be protecting large businesses rather than consumers.[104] Consumers can, and do, suffer out of pocket losses, particularly with new account fraud, but it is unclear how great they must be to constitute substantial injury. Businesses, in general, are capable of protecting themselves against injury. For example, credit card companies include data security requirements in their contracts with merchants. If they do not require more or do not enforce these requirements more aggressively, yet bear the economic consequences of inadequate data security (as is the case with credit card number theft) basic economic logic would suggest that it is because the credit card companies believe that they have struck the optimal balance between costs and benefits. There is little reason to think the FTC knows better.

Determine the appropriate treatment of mitigation costs. It is unclear whether the time and effort required by consumers to mitigate harm, such as by monitoring account charges or replacing credit cards should constitute cognizable harm. Doctrinally, it is unclear whether this

---

[103] *See* Geoffrey A. Manne, Elise M. Nelson & R. Benjamin Sperry, *Gap-Filler or Over-Regulator?: An Empirical Analysis of the FTC's "Common Law" of Data Security* (Working Paper: LEC Law & Economics of Privacy and Data Security Research Roundtable, Dec. 11, 2013).

[104] *See, e.g.,* In re Negotiated Data Solutions, LLC, Dissenting Statement of Commissioner Kovacic, Dkt. No. 051-0094 (2008), at 2, *available at* http://www.ftc.gov/enforcement/cases-proceedings/051-0094/negotiated-data-solutions-llc-matter. ("The Commission's discussion of the UAP liability standard accepts the view that all business enterprises – including large companies – fall within the class of consumers whose injury is a worthy subject of unfairness scrutiny."). *See also* Ohlhausen Bosch Dissent, *supra* note 43, at 3.

should be measured as a form of injury or as part of the inquiry into whether consumers can "reasonably avoid" injury. Logically, if *any* mitigation costs were considered "substantial" injury, the "reasonably avoidable" prong of unfairness would be meaningless, and "injury" would probably be stretched far beyond the boundary of substantiality.

Consider the appropriate extent of specificity. The current *de facto* guidance provided in the Safeguards Rule, while offering some details, nonetheless ultimately rests on operative standards like "reasonable" and "effective." The agency has not, as far as I know, carefully considered whether this is the appropriate amount of specificity and guidance necessary since the Safeguards Rule itself was adopted; certainly this is the case with respect to the appropriate amount of specificity in data security and other fast-paced issues.

Explain reasonable foreseeability. As the FTC expands its data security enforcement efforts into increasingly novel situations, the key question increasingly becomes whether a specific risk was reasonably foreseeable. In at least one closing letter, the FTC explained that the risk of a particular technique for stealing debit card information at cash registers was not reasonably foreseeable, given its sophistication.[105] Yet in recent years the FTC has, among other things, alleged that a small cancer treatment lab should have foreseen the risks posed by peer-to-peer file-sharing software as a potential source of data leakage and taken even more steps than it did to keep such software off its machines[106] – long before the FTC itself issued any formal guidance on such matters[107] and years before the FTC brought an enforcement action against the makers of such software for designing it in such a way as to trick users into over-sharing information.[108] Doctrinally, this question speaks to what the defendants in *Wyndham* have argued is actually the fourth prong of unfairness: causation.[109]

Determine the role of specific company characteristics in deciding outcomes. It is unclear (in large part because the extent of publicly available analysis is so minimal) whether reasonableness depends, under the Safeguards Rule, on the specific characteristics of the company. To the extent that it does, the mechanism is opaque. A well-considered policy statement could identify whether and how particular businesses might avoid inefficient

---

[105] *See* Dollar Tree Closing Letter, *supra* note 102.

[106] In the Matter of LabMD, Docket No. 9357, *available at* http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[107] FEDERAL TRADE COMMISSION, PEER-TO-PEER FILING SHARING: A GUIDE FOR BUSINESS (2010), *available at* http://www.business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.

[108] In the Matter of Frostwire and Angel Leon, No. 111-cv-23643, *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon.

[109] Section 45(n) provides that "[t]he Commission shall have no authority … to declare … an act or practice … unfair unless the act or practice **causes or is likely to cause** substantial injury to consumers…." [Emphasis added].

implementation of the FTC's data security standards based on particular company characteristics. Similarly, more rigorous guidance could better ensure that the duty of care imposed on businesses is appropriate to their size and degree of sophistication, as well as to the security threats at issue.

Consider whether FTC action is necessary to fulfill shortcomings in common law and private ordering. Often, private actions under the common law, state-level statutes, and even federal statutes already cover harms that FTC actions are supposed to ameliorate. Contract remedies, negligence, and negligent misrepresentation, among others, have been used successfully by private litigants, especially when actual harm is plead.[110] Before the FTC acts to protect consumers from harms that have been dealt with elsewhere, it should consider whether the additional, marginal effect of its own enforcement is actually necessary.

Process Issues

Consent Decrees

In some areas of law, most notably privacy, data security, and high-tech product design, the FTC operates almost entirely by settling enforcement actions in consent decrees. Consent decrees, generally with 20-year terms, are also increasingly becoming a tool for informal policymaking, allowing the Commission to require individual companies to agree to things that are not required by law and thus might more appropriately be addressed on a general basis through the FTC's essentially forgotten Magnuson-Moss rulemaking process. This is particularly true in the high-tech sector and on issues such as privacy. With nearly every major large technology company operating under a consent decree, many have asked whether the FTC is moving towards a form of regulation in which its discretion will be even less constrained, as companies face additional pressure to settle alleged violations of consent decrees because they face monetary penalties (unavailable in Section 5 cases) and even worse public relations fallout than for violations of Section 5.

It is unclear what limits (if any) exist on the FTC's discretion in setting the terms of consent decrees and thus on its ability to make policy via consent decree, such as by requiring "privacy by design" or "security by design" or, in the case of Apple, "industrial design by the FTC's design."

Because the standards for determining whether a company has violated a consent decree differ from those required to establish a Section 5 violation, and because the legal standard is

---

[110] *See generally* Sasha Romanosky, et al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL L. STUD. 74 (2014).

much lower, the FTC may be using consent decrees, unmoored from the requirements of Section 5 or its own Unfairness and Deception Policy Statements, to circumvent the constraints established by its own Policy Statements and by Congress.

Moreover, bringing these companies under consent decrees, and then treating future conduct as a violation of those decrees even when not clearly related, allows the FTC to invent the very power Congress has refused to give it: a blanket authority to issue civil penalties. In general, the FTC may not impose penalties for first-time violations of Section 5, only for violations of consent decrees. In 2010, the FTC lobbied aggressively for general civil penalty authority as part of the financial regulatory overhaul, but was rebuffed by Congress – and for good reason: the looming threat of monetary penalties would significantly discourage companies from innovating in areas where technology may unsettle user expectations, and further aggravate the problem of companies tending to settle FTC complaints, rather than litigate. The result would be both a decline in innovation, thus harming consumers; a freer hand for the FTC in pushing the boundaries of consumer protection law beyond what Congress intended; and even less guidance as to the boundaries of the FTC's so-called common law of consumer protection.

There are further problems. In cases where the agency does act, the FTC's complaints describe numerous potential problems but offer few insights into which ones were particularly important to the FTC's decision to bring an enforcement action. For example, the FTC's apparent desire to avoid suggesting that any one step is the key to information security has trumped the need for guidance to the regulated community about what is important and what is not required. Such lack of guidance could well violate judicial requirements that agencies must, to satisfy constitutional standards of due process, provide "fair notice" of their policies, although that judicial doctrine may be underdeveloped.[111]

In many instances consent agreements are efficient and effective: No one is saying that the FTC should have to litigate every case, most cases or even very many cases. But there is a world of difference between having very nearly *no* litigated cases and having *some*. Given the reality that companies are reluctant to litigate, the obvious place to begin addressing the guidance problem is with the complaints and consent agreements themselves. For example, the FTC could explain more of its legal analysis in its complaints. In an amicus brief in the *Wyndham* case, Gus Hurwitz, Paul Rubin, Berin Szoka, Todd Zywicki and I have argued that the FTC's unfairness complaint in that case (and in data security cases more generally) may not satisfy even the minimum pleading requirements laid out in *Twombly* and *Iqbal*; further, the FTC fails to fulfill the particularity requirements Federal Rule of Civil Procedure 9(b), governing cases that "sound in fraud" (which would seem to, and ought to, include deception).[112] In

[111] *See* Wyndham Amicus Brief, *supra* note 100, at 6-12.

[112] *See id.* at 12-20.

addition, the FTC could issue competitive impact statements with each settlement, including a fuller discussion of the agency's reasoning, the importance of particular facts and legal arguments, and clarification of general principles.

The problem of the excessive use of consent decrees at the agency is exacerbated by its administrative procedures, which create a fundamental imbalance between the agency and the businesses it regulates. As Commissioner Wright noted in his speech introducing his UMC Statement:

> The uncertainty surrounding the scope of Section 5 is exacerbated by the administrative procedures available to the Commission for litigating unfair methods claims. This combination gives the Commission the ability to, in some cases, take advantage of the uncertainty surrounding Section 5 by challenging conduct as an unfair method of competition and eliciting a settlement even though the conduct in question very likely would not violate the traditional federal antitrust laws. This is because firms typically will prefer to settle a Section 5 claim rather than going through lengthy and costly administrative litigation in which they are both shooting at a moving target and have the chips stacked against them. Such settlements only perpetuate the uncertainty that exists as a result of ambiguity associated with the Commission's Section 5 authority by encouraging a process by which the contours of the Commission's unfair methods of competition authority are drawn without any meaningful adversarial proceeding or substantive analysis of the Commission's authority.[113]

Or as Commissioner Wright highlighted in his dissent in *Nielsen/Arbitron*:

> Whether parties to a transaction are willing to enter into a consent agreement will often have little to do with whether the agreed upon remedy actually promotes consumer welfare. The Commission's ability to obtain concessions instead reflects the weighing by the parties of the private costs and private benefits of delaying the transaction and potentially litigating the merger against the private costs and private benefits of acquiescing to the proposed terms.... Put simply, where there is no reason to believe a transaction violates the antitrust laws, a sincerely held view that a consent decree will improve upon the post-merger competitive outcome or have other beneficial effects does not justify imposing those conditions. Instead, entering into such agreements subtly, and in my view harmfully, shifts the Commission's mission from that of antitrust enforcer to a much broader mandate of "fixing" a variety of perceived economic welfare-reducing arrangements.
>
> Consents can and do play an important and productive role in the Commission's competition enforcement mission.... However, consents potentially also can have a

[113] Wright, *Section 5 Recast*, *supra* note 42, at 10.

> detrimental impact upon consumers. The Commission's consents serve as important guidance and inform practitioners and the business community about how the agency is likely to view and remedy certain mergers. Where the Commission has endorsed by way of consent a willingness to challenge transactions where it might not be able to meet its burden of proving harm to competition, and which therefore at best are competitively innocuous, the Commission's actions may alter private parties' behavior in a manner that does not enhance consumer welfare. Because there is no judicial approval of Commission settlements, it is especially important that the Commission take care to ensure its consents are in the public interest.[114]

The pseudo-common law of un-adjudicated settlements, lacking any doctrinal analysis that the FTC has developed under its unfairness authority, simply doesn't provide sufficient grounds to separate the fair from the unfair.[115]

Perhaps most significantly in this regard, the FTC's so-called "common law" decisions identify, at best, only what conduct in specific instances *violates* the law; they do not identify what conduct does *not* violate the law. Real common law, by contrast, provides insights into both – offering guidance to firms regarding not only specifically proscribed conduct but also the scope of conduct in which they may operate without fear of liability. Consent decrees tell us, for example, that "invitations to collude" and "deception in standard setting" are violations of Section 5. And thus they are potentially useful guidance for that conduct. But they tell us very little to nothing about the *next* type of conduct that will be prosecuted under Section 5.

Instead, the FTC's current approach to its unfairness enforcement denies companies "a reasonable opportunity to know what is prohibited" and thus to follow the law. The FTC has previously suggested that its settlements and Congressional testimony offer all the guidance a company would need, as when Chairwoman Ramirez claimed that:

> Section 5 of the FTC Act has been developed over time, case-by-case, in the manner of common law. These precedents provide the Commission and the business community with important guidance regarding the appropriate scope and use of the FTC's Section 5 authority.[116]

---

[114] Wright, *Nielsen* Dissent, *supra* note 16, at 6-7.

[115] *See* Wyndham Amicus Brief, *supra* note 100, at 6-7.

[116] Ramirez Questions for the Record, *Hearing before the S. Comm. on the Jud. Subcomm. on Antitrust, Competition Pol'y and Consumer Rights: "Oversight of the Enforcement of the Antitrust Laws"* (Apr. 16, 2013), *available at* http://www.judiciary.senate.gov/resources/documents/113thCongressDocuments/upload/041613QFRs-Ramirez.pdf. *See also Hearing before S. Comm. on the Jud. Subcomm. on Antitrust, Competition Pol'y and Consumer Rights: Standard Essential Patent Disputes and Antitrust Law* (statement of Federal Trade Commission, Jul. 30, 2013), *available at* http://www.judiciary.senate.gov/pdf/7-30-13MunckTestimony.pdf.

But settlements (and testimony summarizing them) do not in any way constrain the FTC's subsequent enforcement decisions. They cannot alone be the basis by which the FTC provides guidance on its UMC authority because, unlike published guidelines, they do not purport to lay out general enforcement principles and are not recognized as doing so by courts and the business community. It is impossible to imagine a court faulting the FTC for failure to adhere to a previous settlement, particularly because settlements are not readily generalizable and bind only the parties who agree to them.[117] As we put it in our *Wyndham* amicus brief:

> Even setting aside this basic legal principle, the gradual accretion of these unadjudicated settlements does not solve the vagueness problem: Where guidelines provide cumulative analysis of previous enforcement decisions to establish general principles, these settlements are devoid of doctrinal analysis and offer little more than an infinite *regress* of unadjudicated assertions.[118]

Rulemaking is generally preferable to case-by-case adjudication as a way to develop agency-enforced law because rulemaking both reduces vagueness and constrains the mischief that unconstrained agency actions may cause. As the Supreme Court noted in *SEC v. Chenery Corp.*:

> The function of filling in the interstices of [a statute] should be performed, as much as possible, through this quasi-legislative promulgation of rules to be applied in the future.[119]

Without Article III court decisions developing binding legal principles, and with no other meaningful form of guidance from the FTC, the law will remain vague – perhaps even unconstitutionally so.[120] And the FTC's approach to enforcement also allows the FTC to act both arbitrarily and discriminatorily—backed by the costly threat of the CID process and Part III adjudication. This means a company faces two practically certain defeats—before the administrative law judge and then the full Commission, each a public relations disaster.

Reports & Workshops as Informal Rulemakings

Information-gathering is essential both to inform the FTC's law enforcement efforts and as an end unto itself, to inform the larger policy debates about important issues at the agency, including notably privacy and data security. The FTC has held a series of workshops and issued

---

[117] *See, e.g.*, Altria Group, Inc. v. Good, 555 U.S. 70, 89 n.13 (2008) (noting a FTC "consent order is… only binding on the parties to the agreement").

[118] Wyndham Amicus Brief, *supra* note 100, at 8-9.

[119] SEC v. Chenery Corp., 332 U.S. 194, 202 (1947).

[120] *See* Wyndham Amicus Brief, *supra* note 100, at 6-12.

a string of reports since 1996.[121] Together, these provide an invaluable narrative of the history of consumer privacy in the U.S.

But the purpose of the reports has clearly shifted, from descriptive to prescriptive. Now, rather than describe the state of the art or issues raised by technological change, or even summarizing FTC enforcement actions, the agency's reports routinely assert what companies "should" do, setting best practices that the agency turns into more than mere recommendations. These "recommendations," most recently, for "privacy by design" and "security by design," are not technically legally binding. But the FTC has pushed companies to adopt them through a combination of public pressure from the Commission's large bully pulpit, treating them as unofficial legal standards in enforcement actions,[122] requiring companies to agree to them when settling enforcement actions, and heavily pushing their incorporation into multistakeholder standard-setting processes. In short, the workshop-and-report process has become a functional part of the FTC's extra-legal formulation of "soft law" that is not clearly grounded in the agency's Section 5 legal authority or in any systematic or rigorous economic analysis. Indeed, this process has effectively allowed the FTC to circumvent the procedural safeguards imposed by Congress in the special Magnuson-Moss rulemaking authority for Section 5.

The Role of the Bureau of Economics

Implementing more and better economic analysis at the FTC should begin with a consideration of how the agency can make better use of the considerable economic expertise in its Bureau of Economics (BE). The FTC is an unusual agency in that it has a large staff of economists; it should leverage that capacity to guide all of its work. That means the FTC should better employ its economics expertise in a meaningful way in consumer protection issues.

Relatedly, cost-benefit analysis of the sort regularly employed by BE should be more widely practiced by the Commissioners in their decision-making and policy analysis. For example, ongoing privacy discussions have been largely devoid of any rigorous cost-benefit analysis.

---

[121] *See, e.g.*, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at B-1 (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (timeline listing major FTC privacy actions and identifying workshops and reports). *See also* "Legal Resources > Reports and Workshops" http://www.business.ftc.gov/legal-resources/8/34.

[122] *See* In *Wyndham*, for instance, the FTC argued that parties had sufficient notice in part because of the business guidance brochure the FTC published. *See* FTC v. Wyndham, Civil Action No. 13-1887, at 17 (D.N.J. Apr. 7, 2014), *available at* http://epic.org/privacy/big-data/ftc-v-wyndham-opinion.pdf.

This should be rectified, and institutional reforms put in place to ensure that cost-benefit analysis is both rigorous and a meaningful check on agency discretion.

The Bureau of Economics has long shaped the Bureau of Competition's implementation of the antitrust laws, both by having a formal role in competition enforcement and by having a leading role in writing the antitrust guidelines co-authored by the FTC and Department of Justice. But what is BE's role in consumer protection matters, and what should it be? Indeed, what is the role of economics as a discipline in limiting the FTC's broad discretion to define UDAP, and in ensuring that the FTC's UDAP efforts do not inadvertently harm competition?

As the FTC increasingly uses its deception authority beyond enforcement of traditional marketing claims to enforce codes of conduct, FAQs, help files and other informal statements, it is testing the presumption of materiality that once helped to ensure that consumers got the benefit of the bargain promised them. Economic analysis, and BE in general, can and should play a significant role in shaping the Commission's emerging, expanded doctrine of materiality.

The Unfairness Policy Statement clearly defines consumer injury as the lodestar of Section 5 and demands cost-benefit analysis by requiring that the FTC weigh injury against countervailing benefits to consumers or to competition. Yet, with scant litigation of unfairness cases (both UAP and UMC), it is not clear that the FTC is engaging in much cost-benefit analysis in practice. The Apple case, discussed above, raises serious concerns in this regard, and it is apparent that the requisite economic analysis was simply absent in the majority's holding in that case, as Commissioner Wright notes in his dissent:

> To support the complaint and consent order the Commission issues today requires evidence sufficient to support a reason to believe that Apple will undersupply guidance about its platform relative to the socially optimal level.... Staff has not conducted a survey or any other analysis that might ascertain the effects of the consent order upon consumers.... The absence of this sort of rigorous analysis is made more troublesome in the context of a platform with countless product attributes and where significant consumer benefits are intuitively obvious and borne out by data available to the Commission.[123]

And on the particularly thorny question of the effect of the FTC's decisions — enforcement and policy-making alike — economic analysis and input from BE should play a significant role in assessing the impact of regulation on innovation.

---

[123] Wright *Apple* Dissent, *supra* note 85, at 14.

HSR Amendments

Last year, over Commissioner Wright's dissent, the FTC approved amendments to its HSR rules[124] that, as Wright summarizes in his dissent,

> Establish, among other things, a procedure for the automatic withdrawal of an HSR filing upon the submission of a filing to the U.S. Securities and Exchange Commission announcing that the notified transaction has been terminated.[125]

As Commissioner Wright pointed out in his Concurring Statement to the Notice of Public Comment before the rules were adopted:

> The proposed rulemaking appears to be a solution in search of a problem. The Federal Register notice states that the proposed rules are necessary to prevent the FTC and DOJ from "expend[ing] scarce resources on hypothetical transactions." Yet, I have not to date been presented with evidence that any of the over 68,000 transactions notified under the HSR rules have required Commission resources to be allocated to a truly hypothetical transaction. Indeed, it would be surprising to see firms incurring the costs and devoting the time and effort associated with antitrust review in the absence of a good faith intent to proceed with their transaction.
>
> The proposed rules, if adopted, could increase the costs of corporate takeovers and thus distort the market for corporate control. Some companies that had complied with or were attempting to comply with a Second Request, for example, could be forced to restart their antitrust review, leading to significant delays and added expenses. The proposed rules could also create incentives for firms to structure their transactions less efficiently and discourage the use of tender offers. Finally, the proposed new rules will disproportionately burden U.S. public companies; the Federal Register notice acknowledges that the new rules will not apply to tender offers for many non-public and foreign companies.
>
> Given these concerns, I hope that interested parties will avail themselves of the opportunity to submit public comments so that the Commission can make an informed decision at the conclusion of this process.[126]

---

[124] Premerger Notification; Reporting and Waiting Period Requirements, 78 Fed. Reg. 41293 (Jul. 10, 2013), *available at* http://ftc.gov/os/fedreg/2013/06/130628hsrfinalrulefrn.pdf.

[125] Dissenting Statement of Commissioner Joshua D. Wright Regarding Amendments to Hart-Scott-Rodino Rules, FTC Matter No. P989316 (Jun. 28, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/dissenting-statement-commissioner-joshua-d.wright/130628hsrstmtwright.pdf. For my previous discussion of the proposed amendments and the circumstances surrounding their adoption, see Geoffrey Manne, *Josh Wright Begins Making His Mark at the FTC by Pushing Cost-Benefit Analysis*, TRUTH ON THE MARKET (Feb. 4, 2013), http://truthonthemarket.com/2013/02/04/josh-wright-begins-making-his-mark-at-the-ftc-by-pushing-cost-benefit-analysis/.

Unfortunately the amendments were adopted without any evidence whatever to suggest they were needed or would be helpful in any way, thus running roughshod over the basic "principle of good governance that federal agencies should issue new regulations only if their benefits exceed their costs."[127]

As it happens, the single comment received by the Commission on the proposed rule supported Wright's views:

> Although the rule may prevent such inefficiency in the future, it would also require companies to incur substantial costs in premerger negotiations and resource allocation while waiting for FTC approval during the HSR period. Currently, firms can avoid such costs by temporarily withdrawing offers or agreements until they are assured of FTC approval. Under the proposed rule, however, doing so would automatically withdraw a company's HSR filing, subjecting it to another HSR filing and filing fee.[128]

It must be counted a straightforward abdication of sensible principles of economic analysis and good governance that these amendments were adopted without any evidence to support them.

Economic analysis at the FTC should not be confined only to competition policy nor only to substantive decision-making. Instead, it can and should govern the full range of the Commission's decisions. Consumers may be harmed just as much by faulty process as by bad substantive decision-making. As Commissioner Wright recently noted:

> When people think about the role that economics plays in antitrust, the first thing they think of is economic analysis aimed at identifying the competitive effects of some business transaction or conduct. I do not think my background in economics necessarily distinguishes what I do from the way others approach problems when evaluating a transaction or conduct, because everybody relies upon economics when approaching those problems—the economics is part of the law.
>
> The bigger difference, in my view, is that economics provides a framework to organize the way I think about issues beyond analyzing the competitive effects in a particular case, including, for example, rulemaking, the various policy issues facing the Commission, and how I weigh evidence relative to the burdens of proof and production.

---

[126] Wright Concurrence in Notice of Public Comment for Proposed HSR Rules, http://www.ftc.gov/os/2013/02/130201hsrnprm-jwrightstmt.pdf.

[127] Dissenting Statement of Commissioner Joshua D. Wright Regarding Amendments to Hart-Scott-Rodino Rules, *supra* note 125, at 1.

[128] Comment of Kenneth Hsu on Comments on proposed amendments to the premerger notification rules, at 1, *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2013/03/564158-00002-85843.pdf.

> Almost all the decisions I make as a Commissioner are made through the lens of economics and marginal analysis because that is the way I have been taught to think.[129]

Some Suggestions for Reform

Instead of asserting what companies should do, the FTC needs to offer more guidance on what it thinks its legal authority means – which is ultimately a matter of economic analysis. And the Commission can't just ignore or revoke those limiting principles when they become inconvenient. A more significant and better-defined role for economics, and thus the agency's Bureau of Economics, could provide some degree of internal constraint. That's a second-best to the external constraint the courts are supposed to provide. But it could at least raise the cost of undertaking enforcement actions simply because three Commissioners — or a few staff lawyers — think they're helping consumers by making an example of a particular company.

One easy place to start would be holding a comprehensive workshop on data security and then issuing guidelines – not merely recommendations, but actual analyses of the FTC's legal authority and the way it has been applied in past cases, *i.e.*, something more akin to the antitrust guidelines than the FTC's various hortatory reports. The FTC has settled more than 50 data security cases but has provided scant guidance, even though data breaches and the identity thefts they cause are far and away the top subject of consumer complaints. The goal wouldn't be to prescribe what, specifically, companies should do but how they should understand their evolving legal duty. For example, at what point does an industry practice become sufficiently widespread to constitute "reasonable" data security, or when does a particular threat become reasonably foreseeable?

More ambitiously, the FTC could use its unique power to enforce voluntary commitments to kick start new paradigms of regulation. That could include codes of conduct developed by industry or multistakeholder groups as well as novel, data-driven alternative models of self-regulation. For example, Uber, Lyft and other app-based personal transportation services could create a self-regulatory program based on actual, real-time data about safety and customer satisfaction. The FTC could enforce such a model — if Congress finally makes common carriers subject to the FTC Act. The same could work for online education, Airbnb and countless other disruptive alternatives to traditional industries and the regulators they've captured.

Finally, the FTC could do more of what it does best: competition advocacy — like trying to remove anticompetitive local government obstacles to broadband deployment. The FTC has earned praise for defending Uber from regulatory barriers taxicab commissions want to

---

[129] Interview with Joshua Wright, *supra* note 26.

protect incumbents. That's the kind of thing a Federal Technology Commission ought to do: stand up for new technology, instead of trying to make "it turn out according to plan."

TECH FREEDOM

Comments of
Berin Szoka, President
TechFreedom

on

"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

A Preliminary FTC Staff Report of the
Bureau of Consumer Protection,
Federal Trade Commission

February 18, 2011

Federal Trade Commission Chairman Jon Leibowitz has made privacy the signature issue of his Chairmanship. With his seven-year term on the Commission ending this September,[1] it is understandable that he should feel a sense of urgency to establish a clear legacy in this area by publishing a final version of this preliminary Staff Report[2] before he leaves office—or to help bolster his case that President Obama should re-nominate him, and the Senate should re-confirm him, for a second term on the FTC, so he can stay on as Chairman. Some might blush to speak of such things in agency filings, but there is no shame in acknowledging this reality, and doing so need not impugn the motives of the Chairman or the many dedicated FTC staffers who have worked so hard for so long on this Report.

Indeed, there is much to praise in the FTC Staff Report: Sections II-IV provide an invaluable survey of the history of privacy regulation in the U.S. and the state of the recent debate over privacy in the non-governmental sector, while the "Proposed Framework" in Section V does a commendable job of outlining, as Commissioner Rosch puts it in his separate statement, "a number of 'best practices' that private firms should adopt from the get-go in order to protect privacy."[3] This report has great value in outlining how "Privacy by Design" can actually be implemented by companies to improve privacy practices, both independently and in conjunction with broader self-regulatory efforts.

---

1 *See* Federal Trade Commission, Jon Leibowitz, Chairman, http://www.ftc.gov/commissioners/leibowitz/index.shtml (last modified Feb. 17, 2011).

2 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, Dec. 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (hereinafter "Staff Report").

3 Staff Report, *supra* note 2, at E-2-3, n. 4 (citing report at v, 39, 40-41, 43-52).

I am particularly pleased that FTC staff has not, as many regulatory advocates proposed at FTC Privacy Roundtables and in written comments, abandoned the concept of opt-out in favor of highly restrictive opt-ins for the collection and use of data about consumers. Indeed, whatever else may be said about the "Do Not Track" mechanism endorsed in the Staff Report, it is, in principle, an affirmation of the argument made by defenders of opt-out that enhancing user choice through technological innovation is superior to imposing restrictive defaults.

For these reasons, the Staff Report could make a fine legacy for any FTC Chairman—one that could earn him plaudits from many corners. But in other respects, the Report raises cause for concern. These comments elaborate on the following concerns:

1. **Regulation v. Best Practices**. As Commissioner Rosch notes, however desirable the best privacy practices outlined by the Report might be, "that does not mean that firms should be mandated *de jure* (*i.e.*, by legislation) to adopt them or that firms should be required to do so *de facto* (*i.e.*, that large, well-entrenched firms engaging in "self-regulation" should dictate what the privacy practices of their competitors should be)."[4]
2. **FIPPS**. In particular, the Fair Information Practice Principles (FIPPS) may offer a fine conceptual framework by which businesses can protect the privacy of their users, but they were developed to limit government access to particularly sensitive data (about health) and are therefore not an appropriate framework for dealing with the trade-offs inherent in regulating privacy in general.
3. **The FTC's Authority**. The FTC has not made a clear case that its existing statutory authority to punish unfair and deceptive trade practices is inadequate to protect consumers. The FTC should, as Commissioner Rosch urges, make fuller use of its existing authority. If the agency requires more resources to use that authority effectively, it should request additional appropriations from Congress before seeking more additional powers.
4. **Regulatory Capture**. The FTC must recognize that its interventions in the market, however well intentioned, will always be subject to "capture" by incumbents as weapons against their competitors.
5. **"Do Not Track**." A "Do Not Track" mechanism could, in principle, be an excellent example of how better user empowerment tools can enhance consumer sovereignty and thus decrease the need for paternalistic interventions. Yet once again, it does not automatically follow that government should mandate the use or design of such a mechanism. Technical mandates for "Do Not Track" would, especially at this early stage, amount to having government design the "market for privacy." It would be better for policymakers to let this tool continue to evolve—and let a marketplace between privacy-sensitive users and publishers emerge. The FTC should, however, use its existing authority to hold companies to their promises to respect "Do Not Track."
6. **Costs & Trade-Offs**. Before issuing a final report, the FTC needs much better data about the economic consequences of its proposals in terms of revenue for ad-supported

[4] *Id*.

media and how that revenue is distributed, potential costs to innovation, and the broader competitive landscape of the Internet ecosystem.

7. **Free Speech**. The consequences of regulating the data-based Internet ecosystem are measured not merely in dollars and cents, or in lost innovation, but in terms of expression, speech, media and journalism. Yet the First Amendment has been almost entirely absent from these discussions.
8. **The Rush**. Most of all, I worry that these and other concerns raised in this proceeding, as well as in the comments on the Commerce Department's Privacy Green Paper,[5] cannot be given the attention they deserve between now and September. The FTC should, in general, refrain from calling for increased regulation or new grants of statutory authority in the Final Report. Future arguments for new powers should be made only after addressing the concerns expressed above.

Some will, no doubt, dismiss these concerns as stalling tactics. Yet this would be as unfair as it would be for those concerned about the implications of regulation to dismiss the desire for enhanced consumer sovereignty by refusing to engage in a serious conversation about enhanced choice mechanisms like "Do Not Track."

Instead, my concerns are grounded in a firm belief that sound policymaking can be reduced to a single question: *"And then what?"* What do we imagine will the first order consequences of the various changes the FTC is proposing companies make—or perhaps be required by law to make—be to the Internet ecosystem? If the purpose of a "Do Not Track" mechanism is to create a market for privacy users to essentially, but simply and seamlessly, negotiate with websites over how to fund content, how do we imagine that marketplace will work? Indeed, how would that marketplace evolve under the more elaborate user choice mechanisms recently released by Microsoft or called for by the FTC?

These three, deceptively simple words—"And then what?"—make much the same point the Nobel Prize-winning economist F.A. Hayek made when he remarked in *The Fatal Conceit*, his damning treatment of top-down government planning, that "[t]he curious task of economics is to demonstrate to men how little they really know about what they imagine they can design."[6]

So, how much do we really know about the framework for governing data use the FTC has outlined in its Staff Report? What will be its costs, its effects on competition, its various other unintended consequences? I detail some of these specific concerns below, but readers will find many other concerns more ably expressed in comments filed in this proceeding by those with what Hayek would have called the best "local knowledge"—the technical experts (generally at companies) who are closest to these details.

---

[5] Department of Commerce Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, Dec. 16, 2010, http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf (hereinafter "Green Paper").

[6] F.A. HAYEK, THE FATAL CONCEIT: THE ERRORS OF SOCIALISM (W. W. Bartley III, ed. 1988)

I. The Harm Standard & the FTC's Framework

"Fools rush in where Angels fear to tread."[7] But Commissioner Rosch isn't one to rush: He has been a reliable voice of caution on the Commission, who is willing to embrace change (for example, the "Do Not Track" mechanism)—but not recklessly. His separate statement hits the nail on the head: Most of what the Staff Report recommends as "best practices" are, indeed, desirable—"But that does not mean that firms should be mandated *de jure* (*i.e.*, by legislation) to adopt them or that firms should be required to do so *de facto* (*i.e.*, that large, well-entrenched firms engaging in 'self-regulation' should dictate what the privacy practices of their competitors should be)."[8] His explanation of the adequacy and flexibility of the FTC's existing framework bears repeating here:

> As a guide to Congress about what privacy protection law should look like, the Report is flawed. First, insofar as the Report suggests that a new framework for consumer privacy should replace "notice" (or "harm") as the basis for Commission challenges relating to consumer privacy protection, that is unnecessary. ***A privacy notice that is opaque or fails to disclose material facts (such as the fact that consumer information may be shared with third parties) is deceptive under Section 5*** [of the Federal Trade Commission Act]. That is particularly true if the sharing of the information may cause tangible harm. Moreover, Section 5 liability could not be avoided by eschewing a privacy notice altogether both because that would generally be competitive suicide and because that course would be deceptive in that it would entail a failure to disclose material facts ….
>
> In short, to the extent that privacy notices have been buried, incomplete, or otherwise ineffective—and they have been—the answer is to enhance efforts to enforce the "notice" model, not to replace it with a new framework.[9]

Another example of how the FTC's existing authority could be used more effectively bears emphasis. As Google noted in its Comments on the FTC Green paper, the "FTC has its own inquiry authority, even absent evidence of a violation, and its investigatory authority also serves what is effectively an audit function. As its track record demonstrates, the FTC utilizes its existing authority to ensure that companies are abiding by their fair information practice obligations and representations."[10] This is especially important given the emphasis placed by the Staff Report on the implementation of Privacy by Design and the use of Privacy Impact Assessments—both things which are susceptible to audits.

---

[7] Alexander Pope, *An Essay on Criticism*, 1709.

[8] Staff Report, *supra* note 2, at E-2-3, n. 4.

[9] *Id*., at E-1-2. *See also* First FTC Privacy Roundtable, Remarks of J. Howard Beales III, George Washington University, at 296-97.

[10] Google, *Comments of Google Inc.* 8, Jan. 28, 2011, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/FINALCommentsonDepartmentofCommercePrivacyGreenPaper%20%283%29.pdf (hereinafter "Google Comments").

Put simply, no one is arguing that the FTC should do nothing. But the agency should use its existing authority to the maximum extent possible before demanding new authority. There is good reason for caution about expanding the FTC's powers: The FTC is already unique in the vastness of its jurisdiction (over nearly the entire economy) and the flexibility of its powers (to punish "unfair" and "deceptive" trade practices). If untethered from the specific meanings of these terms, and certain procedural safeguards, the agency could essentially become a "second national legislature."[11] Giving the agency vast new powers over the use of data would, as more and more of our economy and society becomes dependent on the collection and use of data, risk repeating the agency's calamitous over-reach in the 1970s: The FTC so thoroughly abused its uniquely vast jurisdiction through an expansive conception of "unfairness" by, among other things, trying to ban advertising to children, that it was dubbed the "National Nanny" by the Washington Post, hardly a Thatcherite bastion.[12]

This is why, while the FTC may plan a valuable role as a partner in facilitating further improvement of privacy practices and technological empowerment of users, the agency should not attempt to play the lead role—as Google's comments on the Department of Commerce's Green paper explain:

> [T]he Department (including through a newly created Privacy Policy Office)—alone or in conjunction with relevant enforcement agencies such as the FTC—can convene working groups and synthesize recommendations to provide clear guidance on industry-specific measures needed to protect consumer privacy in a particular context or industry, and to update those recommendations as technology evolves. ***For this approach to be effective, however, the regulators must participate as an open-minded convener without preconceived assumptions as to the best outcome; otherwise, the process is merely government-driven regulation by another name***.[13]

II. The Role of FIPPS in a Dynamic World

To many in the privacy community, the Fair Information Practice Principles (FIPPS) are the "gold standard of privacy" and any suggestion that they not be enshrined in law to govern all aspects of privacy is nothing short of heresy. While no one would deny their value as a framework by which to conceptualize how to protect privacy, they do not answer the more important and difficult questions of how to reconcile privacy with other competing values in any and various situations facing those who must actually design, implement, evaluate and iterate privacy practices in the real world. Much like religious texts, the FIPPS can have great value, but are also too easily subject to overly orthodox, uncritical application by a priesthood of "true believers"—advocates who genuinely care about privacy and have the noblest of intentions

---

[11] Berin Szoka, The Progress & Freedom Foundation, *How Financial Overhaul Could Put the FTC on Steroids & Transform Internet Regulation Overnight*, Progress Snapshot 6.7, Mar. 2010, http://www.pff.org/issues-pubs/ps/2010/pdf/ps6.7-FTC_on_steroids.pdf.

[12] Editorial, *The FTC as National Nanny*, WASHINGTON POST, Mar. 1, 1978 at A14.

[13] Google Comments, *supra* note 10, at 9 (emphasis added).

about protecting others as consumers and citizens, but who downplay, or ignore, the difficulties of applying their doctrine in a world of competing values.

A. The FIPPS Must Be Applied Contextually, not Literally

Properly understanding the FIPPS requires understanding the assumptions on which they rest—just as studying any text requires an appreciation of its origins and how those translate to the present instance. Limiting access by government to particularly sensitive data (about health) raises a set of concerns for which the demands of FIPPS may well be appropriate. But the Internet is a far cry from the government-dominated healthcare sector of the 1970s. In contrast to the static world of "purpose specification," where "data minimization" means reducing possible harms at little cost, the dynamic world of the Internet is one where the most beneficial uses of data cannot be specified *ab initio* and where the minimization of data collection—the "precautionary principle" approach to privacy—comes at a significant cost.

Thus, for the FIPPS to be useful, they "must be appropriately tailored and relevant for their intended use,"[14] as Google argues—in other words, adapted to reflect the competing values at stake. The Interactive Advertising Bureau offers a simple illustration of the need for such adaptation, depending on the costs and harms at issue:

> [FIPPS'] data quality and integrity requirements are unnecessary in online advertising. The costs associated with building the infrastructure to permit access and correction rights for advertising and marketing data would significantly outweigh the supposed benefits from these rights. Inaccurate advertising and marketing data would at worse result in a less relevant advertising.[15]

B. Application of the FIPPS Must Allow for Ongoing Evolution

Google's comments on the Green Paper detail several outstanding examples of data collected for one purpose that were later used to develop services now used widely and without serious privacy concerns:

> Creative, even serendipitous re-use of collected data has enabled enormous advances in online products and services that enable creativity, education, the creation of businesses, and deeper social and political engagement. In Google's experience alone, purpose-compatible re-use of existing data has delivered enormous value to Google users and led to product improvements such as Gmail's priority inbox, automated spell checking, auto-complete, spam, fraud and virus protection tools, and the development of new services such as FluTrends and Translate. Mechanistic or overly prescriptive purpose specifications, data minimization and collection limitations, or use limitations

---

[14] *Id*. at 6.

[15] Interactive Advertising Bureau, *Letter RE: IAB's Comments* 7, Jan. 28, 2011, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/ACF2DA.pdf.

> would frustrate such economically and socially valuable innovation without protecting consumers from harm.[16]

As Facebook explains in its Green Paper comments, expectations themselves evolve alongside the technologies we use:

> As technology advances, individuals understand that their data may be used or made available in new ways. In the digital world in particular, users have come to understand and even expect that services will evolve and that companies will offer innovative new features that improve the online experience. The Department of Commerce's report, recognizing that creative reuses of existing information can lead to innovation but also cautioning that such innovative reuses should not come at the expense of user privacy, recommends a nuanced approach to the issue—one that weighs the benefits of the particular reuse against the harms and calibrates notice and consent requirements accordingly. Facebook believes that such an approach is necessary in lift of the many examples of reuse that have provided immense benefits to the public while producing little if any discernible harm. [17]

Because the beneficial uses of data co-evolve with privacy expectations, government must be careful not to foreclose innovation by attempting to freeze the status quo—such as by requiring companies to notify users, or receive consent, before ever using data in a new ways. As Facebook notes:

> While transparency is important, it must be implemented with due regard for the rapidly changing nature of online services and the realization that overly restrictive obligations hinder innovation. For example, the FTC recommends that companies obtain affirmative consent from users before using previously collected data in a "materially different manner" than described in an earlier privacy notice. While Facebook agrees that notice and consent may be appropriate for certain changes in data practices, it is essential to avoid interpreting the term "material" too restrictively. A restrictive interpretation could prevent companies from launching new features out of an uncertainty about whether those features would use data in a "materially different manner." Such an interpretation might have prevented features like the caller ID displays and Netflix recommendations described above from ever having been offered—a result that could hurt the future of the digital economy.[18]

---

[16] Google Comments, *supra* note 10, at 7-8

[17] Facebook, Inc., *Letter Re: Commercial Data Privacy and Innovation in the Internet Economy* 7, Jan. 28, 2011, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/FINALCommentsonDepartmentofCommercePrivacyGreenPaper%20%283%29.pdf (hereinafter "Facebook Comments").

[18] *Id*. at 9.

C. The Danger of Regulatory Capture

Attempting to impose a rigid regulatory regime grounded in FIPPS on a dynamic world is particularly dangerous because of the rapid, and accelerating, pace of technological change online. The problem is not simply that government will struggle to keep pace (it certainly will), but that policymakers must necessarily rely on the companies they regulate to understand the basic facts of new technologies and the (privacy) issues they create. As Tim Wu explains in *The Master Switch*, this reliance by regulator on regulatee means that the latter will inevitably attempt to capture regulation by casting narratives that skew to their advantage:

> The government can act only on the basis of what it understands to be established fact. Much of what is called lobbying must actually be recognized as a campaign to establish, as conventional wisdom, the "right" facts, whether pertaining to climate change, the advantages of charter schools, or the ideal technology for broadcasting. Much of the work of Washington lobbyists is simply an effort to control the conversation surrounding an issue, and new technologies are no exception.[19]

It was through such "fact-establishing" that, as Wu explains, the established incumbents of AM radio used the FCC as a weapon against competition by technologically superior FM radio in the 1930s and 40s.

Privacy regulation is no different from any other form of regulation, and is just as likely to be captured by special interests. Commissioner Rosch notes that such regulatory capture will occur not just when the FTC attempts to regulate outright, but also when it attempts to drive self-regulation:

> the self-regulation that is championed in this area …. may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power[20]

The reality of regulatory capture is yet another reason for exercising caution in both regulating and attempting to shape self-regulation.

III. "Do Not Track"

Last week, Rep. Jackie Speier introduced legislation that would require the FTC to establish standards for a "Do Not Track" mechanism and require online data collectors to obey consumer opt-outs through such a tool.[21] In principle, a "Do Not Track" mechanism could enhance consumer empowerment, giving users the capacity to choose for themselves whether they want behavioral advertising. Such user empowerment tools are superior to restrictive defaults

---

[19] TIM WU, THE MASTER SWITCH, at 130 (201).

[20] Staff Report, *supra* note 2, at E-3.

[21] Congresswoman Jackie Speier, Do Not Track Me Online Act, Feb. 2, 2011, http://speier.house.gov/uploads/Do%20Not%20Track%20Me%20Online%20Act.pdf.

based on the paternalistic assumption that users won't make the "right" choice, no matter how easy that choice is to make. (Of course privacy zealots believe the "right" choice is always to minimize the collection and use of data, because data is dangerous.) But, as with so many things, the devil lies in the details. Even supporters of a "Do Not Track" mechanism should recognize that it would be premature for any technological mandate in this area, for three reasons:

First, markets *are* working. In the past, regulatory advocates insisted government must intervene immediately because, they argued, markets had failed to address privacy concerns. But just days before Rep. Speier introduced her legislation, Microsoft and the Mozilla Foundation launched "do-not-track" tools in new versions of their Internet browsers: Internet Explorer 9[22] and Firefox 4,[23] while Google launched a tool as an add-on for Chrome.[24]

Second, the FTC already has the authority to enforce promises made by data collectors to comply with the wishes of users who express a preference not to be tracked via a "Do Not Track" mechanism. Regulatory advocates, of course, will argue that too few companies will make such promises for this marketplace response to be effective and, therefore, that government must not only enforce such promises, but also mandate compliance with users' "Do Not Track" preferences—and also perhaps mandate use of a "Do Not Track" standard by browser-makers. But it is simply too soon to say how this will develop. And even if it does turn out that many data collectors remain silent on honoring "Do Not Track," other technologies such as Microsoft's variant may simply allow users to block *all* content from such data collectors—including tracking code.

In any event, the technical details of a "Do Not Track" mechanism must be allowed to evolve over time. We cannot expect a workable "Do Not Track" mechanism to simply spring into being overnight—much as people imagined, for centuries after Aristotle, that life was capable of "spontaneous generation." Instead, Ultimately, it is the Internet's existing standards-setting bodies (*e.g.*, W3C, IETF), not Congress or the FTC, that have the expertise to resolve such differences and make a "Do Not Track" mechanism work for both consumers and publishers, as well as advertisers and ad networks. Specifically, that will require some degree of standardization of the following, among other things:

- The definition of "tracking";
- The interface by which users activate and configure the "Do Not Track" mechanism; and
- The process by which websites respond to the mechanism and negotiate with users who want to opt-out of tracking for access to content.

---

[22] Sean Hollister, Internet Explorer 9 RC Now Available to Download, Tracking Protection in Tow (Update), Feb. 10, 2011, http://www.engadget.com/2011/02/10/internet-explorer-9-rc-now-available-to-download-tracking-prote/.

[23] *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities*, The Mozilla Blog, Feb. 8, 2011, http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/.

[24] *See* https://chrome.google.com/webstore/detail/hhnjdplhmcnkiecampfdgfjilccfpfoe.

A. Possible Economic Consequences

Jonathan Mayer, of Stanford's Center for Internet & Society, insists that we need not fret about the economic consequences of "Do Not Track" because, among other reasons, behavioral advertising revenue is a relatively small share of total U.S. online advertising spending: just 4%, he insists.[25] But his comparison mixes apples and oranges: The relevant comparison is not behavioral advertising not to total online advertising revenue (including search advertising spending), but to spending on *display* advertising (advertising sold by websites next to their content): Behavioral advertising spending in 2010 represented roughly 20% of total display ad spending and that ratio is expected to grow.[26]

Regardless, as Ben Kunz explains, the question is not merely how much revenue is available for ad-supported media, but how that revenue is distributed:

> Like the publications of the past century, a given website has always been a proxy for an audience target. Alas for the big publishers, good data on audiences has meant that smart marketers could leave big, expensive sites behind. So in perhaps the biggest revolution of Internet marketing, the more data you can collect about today's customers, the cheaper online advertising gets ….
>
> If the FTC pushes Do Not Track through Congress, it will send billions to The Wall Street Journal (NWS), Forbes.com, iVillage.com, and even Bloomberg Businessweek because marketers will be forced to put ad dollars on those sites. In the absence of data, advertisers will have to make assumptions about who reads content. The top content will win.[27]

In other words, adoption of a "Do Not Track" mechanism could have significant consequences for the structure of the media sector. Some, like *Cult of the Amateur* author Andrew Keen, might argue that this redirection of revenue towards larger, better established websites (and offline to traditional media) is desirable to preserve elite, "professional" media. Others would counter, without (necessarily) denying the value of traditional media, that the "Long Tail" of websites disadvantaged by "Do Not Track" represent diversity, creativity and the "laboratories" of media's future (think Huffington Post). The important point is not which side has the better argument, but that such arguments—over picking winners and losers—are the very hallmark of industrial planning.

---

[25] Jonathan Mayer, *Do Not Track Is No Threat to Ad-Supported Businesses*, Jan. 20, 2011, http://cyberlaw.stanford.edu/node/6592.

[26] Network Advertising Initiative, Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf ("Behaviorally-targeted ads accounted for 17.9% of respondents' advertising revenue, with revenue increasing from 16.2% in Q1 to 19.4% in Q4 2009.").

[27] Ben Kunz, *The $8 Billion Do Not Track Prize*, BLOOMBURG BUSINESSWEEK, Dec. 22, 2010, http://www.businessweek.com/technology/content/dec2010/tc20101222_392883.htm.

Mayer insists "[a]d-supported businesses could ask—or possibly require—Do Not Track users to allow third-party behavioral advertising."[28] In other words, he argues that the market will solve this problem—to be precise, the "market for privacy" created by empowering users to forbid websites to use their data for behavioral advertising purposes. Perhaps. But how will that work? And how well?

Again, I am deeply sympathetic to the concept of creating a privacy marketplace. Adam Thierer and I have, from the start of our work, argued for recognition of the value exchange underlying the Internet ecosystem: Publishers offer free content and services and in exchange, users offer a share of their attention (viewing those ads) as well as information about where their attention is likely to go (making those ads more relevant).

Yet we simply do not know how this new marketplace will evolve as today's implicit *quid pro quo* becomes, or is forced to become, explicit. Thus, government must be cautious when it attempts to design that marketplace from the top down through regulation (as would happen under the bill introduced last week by Rep. Jackie Speier). The same is true when government acts more subtly, using the bully pulpit to intimidate industry (as Chairman Leibowitz has essentially done since calling for "Do Not Track" in Congressional testimony last July[29]). Much as I enjoy the rich irony of seeing those who are rarely thought of as free-marketeers essentially asserting that "markets" will simply, and quickly, "figure it out," I am less sanguine. The hallmark of a true free-marketeer is not a belief that markets work perfectly; indeed, it is precisely the opposite: an understanding that "failure" occurs all the time, but that government failure is generally worse, in terms of its full consequences, than "market" failure.

The first part of that lesson comes especially from the work of the economist Ronald Coase, who did more to teach us "how little [we] really know about what [we] imagine [we] can design" than perhaps anyone. Coase won his Nobel Prize for explaining that the way property right are allocated and markets are structured determines the outcome of marketplace transactions. For example, a rule that farmers bear the cost of stopping rancher's cattle from grazing on their farms by constructing fences will produce different outcomes—not merely different allocations of costs—from the opposite rule.

Coase's key insight was that, in a perfectly efficient market, the outcome would not depend upon such rules: To put this in terms of the privacy debate, the choice between, say, an opt-out rule and an opt-in rule for the collection or use of a particular kind of data (essentially a property right) *would have no consequence* because the parties to the transaction (say, website users and website owners) would express their "true" preferences perfectly, effortlessly and costlessly. But, of course, such frictionless nirvanas do not exist. The real world is defined by what Coase called "transactions costs": search and information costs, bargaining and decision costs, policing and enforcement costs.

---

[28] Mayer, *supra* note 25.

[29] Juliana Gruenwald, *FTC Weighs 'Do Not Track' List*, NationalJournal, July 27, 2010, http://techdailydose.nationaljournal.com/2010/07/ftc-weighs-do-not-track-list.php.

The transaction costs of implementing a "Do Not Track" mechanism as something other than pure free-riding (no-cost opt-outs being, ultimately, unsustainable) are considerable: someone must design interfaces that make it clear to the user what their choice means, the user must consume that information and make a choice about tracking, websites must decide how to respond to various possible choices and be able to respond to users in various ways through an interface that is intelligible to users, and so on—all for what might seem like a "simple" negotiation to take place.

These problems are certainly not insurmountable—and, again, with the right engineering and thoughtful user interface design a "Do Not Track" mechanism could well prove a useful tool for expressing user choice. But when we look at the world through Coase's eyes, we begin to understand that how mechanism design can radically can outcomes (in this case, funding for websites. Indeed, the costs of building and operating a market for privacy—measured in time as well as money—could well swamp the value produced by that market. Clearly, website publishers currently write-off ad-blocking as an acceptable loss because it would cost them more to fix the problem (*e.g.*, by charging users who block ads) than they would gain in revenue by doing so. The question is: how high is that threshold? And how much total revenue will be lost even when publishers are able to get *some* users to pay *something*? These are just some of the questions that must be answered before government inserts itself into the evolution of user choice mechanisms.

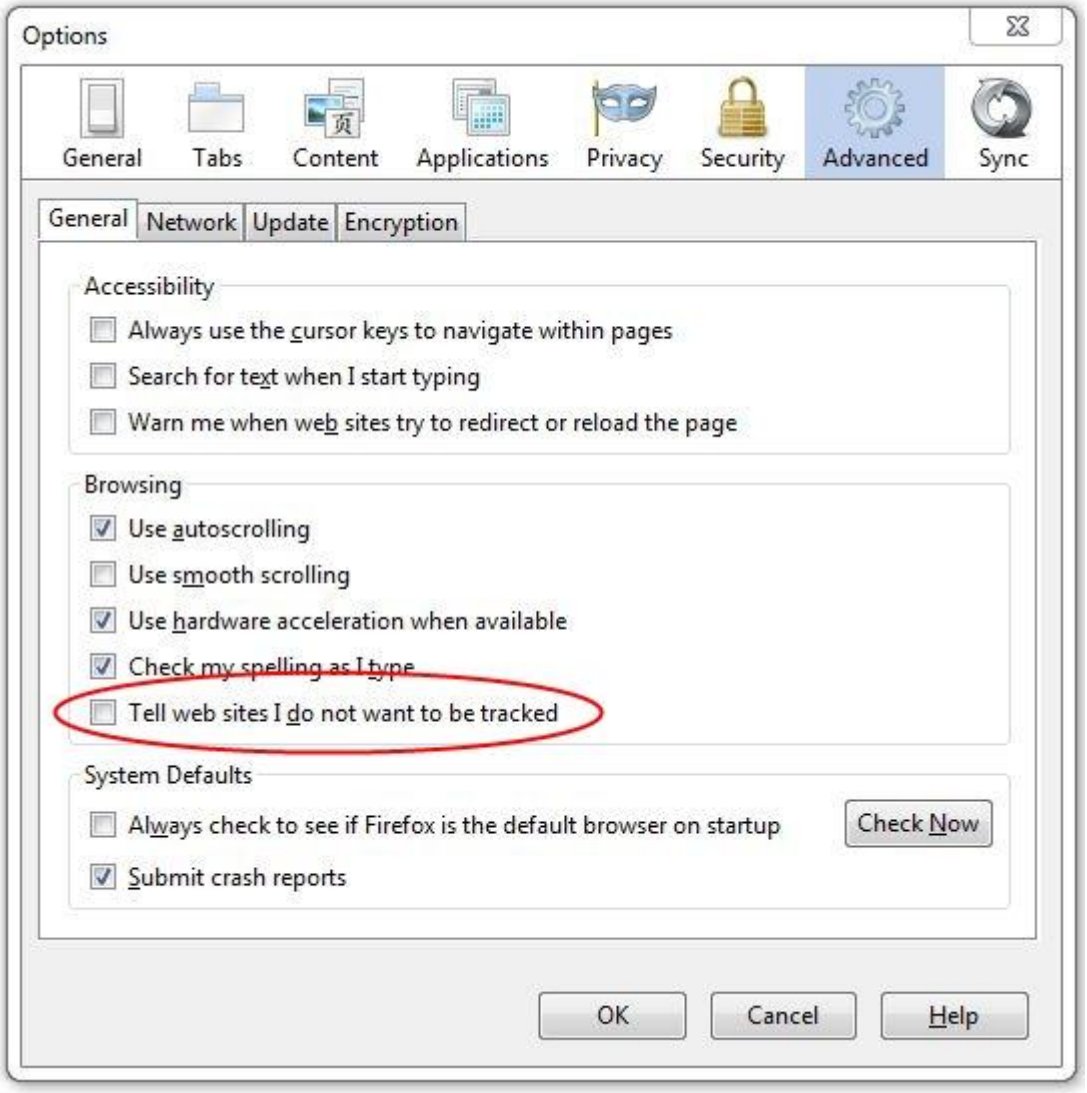
B. More Sophisticated "Do Not Track" Mechanisms

David Vladeck, director of the FTC's Bureau of Consumer Protection, recently made clear in Congressional testimony that the agency ultimately wants a much more granular choice mechanism:

> We therefore urge Congress to consider whether a uniform and comprehensive choice mechanism should include an option that enables consumers to control the types of advertising they want to receive and the types of data they are willing to have collected about them, in addition to providing the option to opt out completely.[30]

In many respects, this is admirable. One of the significant drawbacks to the "Do Not Track" mechanism as implemented in Firefox 4 is that it allows only the expression of a single preference not to be "tracked" across the board—as this screen capture illustrates:

[30] David Vladeck, *Prepared Statement on Do Not Track Before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, United States House of Representatives*, Dec. 2, 2010, http://www.ftc.gov/opa/2010/12/dnttestimony.shtm.



The Electronic Foundation's Green paper comments laud the promise of "Do Not Track" as the first of a potential new generation of user empowerment tools that could give effect to a core FIPPS principle better than a simple legal mandate:

> DNT is just one example of the way that technical measures may improve purpose-related disclosure. DNT is a consumer-expressed preference that says the user's browser information may be used for sending content to the user, but not for recording the user's reading habits. Over time, we believe that similar standards should and will be developed for other kinds of purpose specification.[31]

[31] Electronic Frontier Foundation, Comments to the Department of Commerce Internet Policy Task Force 5-6, http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/ACF2D4.pdf.

But this vision of achieving a core concept of FIPPS—purpose specification—by user empowerment raises significant practical questions. How would more complicated mechanisms actually work? How would websites respond to a wider array of expressions of user intent about what may be done with their data? What would the resulting "marketplace for privacy" look like? What would be the transactions costs of implementing such a marketplace? Would the value generated in such a marketplace sufficiently outweigh transactions costs that the marketplace could continue to sustain ad-supported content and services?

Most pointedly: Why should we believe that the FTC is best suited to answering these difficult questions? I can only hope that the agency will not attempt to answer these questions on its own, but instead rely on the marketplace to develop clearer answers. I will readily join hands with EFF in celebrating user empowerment tools in the privacy context (just as we do in the context of online child protection), but I remain skeptical about the wisdom of having government design such tools, concerned about how well such tools will work, and what their costs will be.

C. Microsoft's "Do Not Load" Mechanism

In the end, Microsoft's IE9 mechanism—which might more accurately be dubbed "Do Not Load,"—might well moot the debate over what tracking means by empowering users to block any content that loads tracking elements whose data collection, use, access or security practices are deemed inadequate by the maker of the Tracking Protection List (TPL) installed by the user.

In principle, such a mechanism is highly compelling for two reasons: First, it is self-enforcing, because the browser simply does not load blacklisted content, rather than relying on a third party to respect a preference expressed in a heading, someone else to detect violations of that preference, an effective punishment, *etc*. As noted above, such a mechanism could someday work in conjunction with a "Do Not Track" mechanism such as that offered by Firefox by blocking content from companies that do not commit to respecting the "Do Not Track" suspenders—a promise the FTC, in turn, would enforce.

Second, the way Microsoft has designed their mechanism is directly analogous to parental control tools that empower the parent to implement their preferences by subscribing to the white list or black list of a trusted third party. In principle, such subscription tools can empower us to make effective tools about complex problems by outsourcing the decisions to trusted third parties—be they large or small, for-profit or non-profit, from corporations to churches to privacy advocacy groups.

Yet "Do Not Load" also raises significant questions. Again, how would a marketplace for privacy actually work to empower publishers to condition access to their content? What would be the costs of building such a marketplace?

And how could such a mechanism be used to manipulate the online market for content and services? After all, "Do Not Load" is simply a powerful tool for blocking content that, in the hands of third parties whose interests do not fully align with users, could be used for great mischief. Microsoft has, wisely, abstained from writing its own TPLs—instead choosing simply

to build the mechanism and let others write TPLs. But what if a TPL were used to block a competitor's content? For example, suppose a computer OEM pre-installed certain TPLs on a browser shipped to the consumer that simply removed page elements served by competitors. This could, in theory, cause Facebook's "Like" button to simply disappear from all websites, for example.

The purpose of this hypothetical is not to trot out a "parade of horribles" that will necessarily follow any "Do Not Track" effort, but to illustrate how little we understand about the real-world consequences of such user mechanisms, and to highlight how dependent those consequences are on mechanism design. Much imaginable market manipulation could be largely addressed by designing an architecture that is transparent to the user. Here are just a few of the questions that ought to be asked about a "Do Not Load" mechanism:

- Could TPLs come pre-installed?
- Would users see the contents of the lists?
- Will users know if/when lists have been updated?
- How will users be informed about the contents of a TPL white list they might be asked to install by a website that is attempting to negotiate with them over access to content?

With so many questions about two radically different user choice mechanisms, it would be premature for the FTC to even begin to contemplate technological mandates in this area—as Rep. Speier's proposed legislation would *require* the agency to do.

D. "Tracking Neutrality"

A very different sort of "neutrality" concern has been raised—over how publishers interact with users. The discussion above concerns how, as a practical matter, websites would respond to privacy-sensitive users who opted out of tracking through the "Do Not Track" header and what the consequences of that back-and-forth might be. A true "privacy marketplace" would be based on empowering users to implement their privacy preferences in a meaningful way, while also empowering website publishers to respond to opt-outs as they see fit.

But this, of course, presumes that websites would be free to condition access to their content on receiving permission to "track" users for advertising purposes or, failing that, charge for their content, or otherwise discourage users from opting out (such as by showing them more ads, or "interstitial" ads with a count-down before they can access a desired page). Harlan Yu, a researcher at Princeton's Center for Information & Society, would allow websites to do so—but only so long as their "discrimination" against privacy-sensitive users was "reasonable":

> nothing would prevent sites from offering limited content or features to users who choose to opt-out of tracking. One could imagine a divided Web, where a user who turns on the x-notrack ["Do Not Track"] header for all HTTP connections—i.e. a blanket opt-out—would essentially turn off many of the useful features on the Web.
>
> By being more judicious in the use of x-notrack, a user could permit silos of first-party tracking in exchange for individual feature-rich sites, while limiting

> widespread tracking by third parties. But many third parties offer useful services, like embedding videos or integrating social media features, and they might require that users disable x-notrack in order to access their services. Users could theoretically make a privacy choice for each third party, but such a reality seems antithetical to the motivations behind Do Not Track: to give consumers an easy mechanism to opt-out of harmful online tracking in one fell swoop.
>
> ***The FTC could potentially remedy this scenario by including some provision for "tracking neutrality," which would prohibit sites from unnecessarily discriminating against a user's choice not to be tracked.*** I won't get into the details here, but suffice it to say that crafting a narrow yet effective neutrality provision would be highly contentious.[32]

Yu likely won't be the only one to suggest such restrictions, which will likely find support from those in the "free culture" movement who generally do not accept that those who produce content, or offer a service, have every right (subject to fair use, consumer deception laws and antitrust) to condition or restrict access to that content/service. The Staff Report itself leaves the door open to such proposals, as Commission Rosch notes—and rightly rejects:

> insofar as the Report could be read as suggesting a ban on "take it or leave it" options (see Report at 60), again, clear and conspicuous disclosure is the most appropriate way to deal with such an option. I question whether such a ban would be constitutional and am also concerned about the impact of a ban on innovation.[33]

This serves merely to illustrate one dimension of the "And then what?" approach policymakers should follow in understanding the many and various consequences of pushing a "Do Not Track" mechanism. Harlan is clearly right about one thing: "Do Not Track," as the title of his blog post says, is "Not as Simple as it Sounds."

E. Metrics for Success

In the end, perhaps the most important question to be asked about "Do Not Track" is: What are the metrics for success? When many "Do Not Track" advocates draw analogies to the "Do Not Call" registry, they imply that success would look similar in both cases: adoption by a majority for users. But, returning to the alternative framework for approaching privacy outlined above, we cannot know what value users really place on privacy until we see their preferences revealed in the marketplace when they must choose from among competing variables. In other words, we really do not know how many people would choose to enact "Do Not Track" when presented with a choice among clear alternatives: allow tracking, move on to another site, or pay some cost in terms of additional advertising, or payment for content. So, how will we know

---

[32] Harlan Yu, *Do Not Track: Not as Simple as it Sounds*, Freedom to Tinker, Aug. 10, 2010, http://www.freedom-to-tinker.com/blog/harlanyu/do-not-track-not-simple-it-sounds (emphasis added).

[33] Staff Report, *supra* note 2, at E-6.

how much adoption is enough? Or will it be the availability of useful tools that matters, regardless of how many people use them? And how will we measure the costs of such mechanism? The FTC has proposed an admirable standard:

> [A]ny such [Do Not Track] mechanism should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value.[34]

What kind of empirical evidence would actually satisfy us that such a standard has been met?

IV. "~~Elvis~~ *The First Amendment* Has Left the Building!"

Whatever government does in regulating the use and collection of data online cannot be done without regard to the First Amendment, because (i) online "privacy" regulation is the regulation of how data flows in the Internet ecosystem, (ii) those data flows are essential to the tailoring, delivery and funding of online speech, and thus (iii) restrictions on the flow of data are, to varying degrees and each in their own ways, restrictions on speech itself. This is not to say that government may do nothing, but that we must understand how any particular proposed government intervention affects online speech, decide what level of First Amendment scrutiny applies, and then ask whether the government has met its burden to satisfy that scrutiny.

Sadly, the First Amendment seems to be almost entirely absent from the general drive towards increased privacy regulation. Nowhere does the FTC staff report mention "free speech" or the "First Amendment."[35] Only Commissioner Rosch mentions concerns about the First Amendment, noting that it might be unconstitutional for the FTC to ban "'take it or leave it' options" by which website publishers would refuse to make their content available unless users accepted tracking.[36] Yes, indeed, dictating to publishers on what terms they may make their content available would be the ad-supported ("free") content world's equivalent of price controls. Turning media providers into public utilities that must provide content as "common carriers" to all visitors, regardless of whether those visitors contribute to the business model that funds free content, would obviously impinge on the First Amendment rights of publishers.

But this is only the most extreme example of a more general First Amendment problem raised by privacy regulations: When government regulates the use of data for advertising purposes, it necessarily affects the funding available to ad-supported publishers, as noted above.

---

[34] Staff Report, *supra* note 2, at 67.

[35] Even the ACLU, perhaps America's most stalwart defender of free speech, seem oblivious to the integral relationship between free speech and the flow of information: The FTC cites their primer *Privacy and Free Speech: It's Good for Business*, which, despite its name is *not* about the relationship *between* privacy and free speech, but about how companies can suffer in the marketplace by invading privacy or interfering with free speech. Staff Report at 45 (citing ACLU, *Privacy and Free Speech: It's Good for Business*, http://www.aclunc.org/docs/technology/privacy_and_free_speech_it's_good_for_business.pdf). While this is, indeed, a core argument that market forces will drive companies to self-regulate, it misses the larger connection between free speech and privacy.

[36] Staff Report, *supra* note 2, at E-6.

More generally, speech and privacy are but two sides of the same coin. After all, what is your "right to privacy" but a right to stop me from observing you and speaking about you?[37] Thus, when government restricts the collection of information, it also restricts the processing and reporting of information—also known as "reporting." This point is commonly recognized, yet few people think through the implications of data regulations for online speech. The simple truth is that online speech is only as effective as it is "targeted" to a particular audience—and that effective "targeting" requires useful data about the likely interests of a potential reader/listener/viewer. This is as true for companies that buy online ads for toothpaste as it is for political candidates and non-profit causes that attempt to reach voters, supporters, donors and volunteers through online media.

If government limits the ability to speak effectively online, whether through direct regulation or indirect pressure, it necessarily implicates the First Amendment. The difficulty facing the FTC in this area lies in the nature of online speech platforms: Past laws regulating the Internet (*e.g.*, COPPA, COPA) have attempted to avoid First Amendment problems by exempting non-commercial websites (and thus avoiding the strict scrutiny standard), but this approach breaks down in a world where online speech flows not from individual websites, but through *platforms*. For instance, if government regulation reduces the data available to target an ad through an ad network or a message through a social network, that regulation necessarily falls on both commercial speakers (the toothpaste ad) and non-commercial speakers (the political or message ad). There is no easy way to "carve out" more highly protected non-commercial speech, because data regulations burden the platforms that carry *all* online speech.

V. An Alternative Framework for Approaching Privacy

So, how *should* policymakers and companies approach privacy, in deciding how to apply FIPPS and other ideas about privacy in the real world? As I argued in my earlier filing on the FTC's Privacy Roundtables,[38] any discussion about regulating the collection, sharing, and use of consumer information online must begin by recognizing the following:

- Privacy is "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."[39]
- As such, privacy is not a monolith but varies from user to user, from application to application and situation to situation.

---

[37] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STANFORD L. REV. 1049 (2000), http://www.pff.org/issuespubs/pops/pop7.15freedomofspeech.pdf.

[38] Berin Szoka, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech,* Comments to the FTC Privacy Roundtables (Dec. 7, 2009), Comment, Project No. P095416, http://www.pff.org/issues-pubs/filings/2009/111009-FTC-privacy-workshop-filing.pdf.

[39] "Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves." Jim Harper, Cato Institute, *Understanding Privacy–and the Real Threats to It*, Cato Institute Policy Analysis No. 520, Aug. 4, 2004, http://www.cato.org/pub_display.php?pub_id=1652.

- *There is no free lunch*: We cannot escape the trade-off between locking down information and the many benefits for consumers of the free flow of information.
- In particular, tailored advertising offers significant benefits to users, including potentially enormous increases in funding for the publishers of ad-supported content and services, improved information about products in general, and lower prices and increased innovation throughout the economy.
- Tailored advertising increases the effectiveness of speech of all kinds, whether the advertiser is "selling" products, services, ideas, political candidates or communities.

With these considerations in mind, policymakers should always look for the "least restrictive" means available to address clear harms—in the broad, but still provable, sense Commissioner Rosch talks about harm. Beyond preventing unfair and deceptive trade practices by the companies that use and collect online data, government can also play a vital role in protecting consumers from real harms that flow from the use of their data, such as the use of personal data to make decisions about credit. Government may even play a proper role in supporting education about privacy risks and promoting technical tools that empower consumers to make more effective decisions about their own privacy—just as it has done with parental empowerment solutions to address concerns about online child safety and protection.

But as in that context, where the courts insist on such a "least-restrictive means" test as a matter of First Amendment doctrine, we have argued consistently for the following layered approach to concerns about online privacy.[40] Government should:

1. ***Erect*** a higher "Wall of Separation between Web and State" by increasing Americans' protection from government access to their personal data—thus bringing the Fourth Amendment into the Digital Age.
2. ***Educate*** users about privacy risks and data management in general as well as specific practices and policies for safer computing.
3. ***Empower*** users to implement their preferences about the real-world trade-offs between privacy and other values as easily as possible.
4. ***Enhance*** self-regulation by industry sectors and companies to integrate with user education and empowerment tools (*e.g.*, respecting evolving consumer choice mechanisms).
5. ***Enforce*** existing laws against unfair and deceptive trade practices as well as state privacy tort laws.

[40] *See, e.g.,* Berin Szoka & Adam Thierer, *Online Advertising & User Privacy: Principles to Guide the Debate*, Progress Snapshot 4.19, Sept. 2008, available at http://www.pff.org/issues-pubs/ps/2008/ps4.19onlinetargeting.html.

VI. Conclusion

The approach I propose above might be called "conservative." In one sense, it is just the opposite: an argument that we must embrace change in a dynamic world, and that we cannot maintain the technological status quo.[41]

But in another sense, this approach does harken back to Edmund Burke's "conservatism" of prudence. Burke, in general, argued against the absolutist radicalism of the French Revolution's Jacobin elements, earning him the caricature as a purely reactionary champion of the status quo and its established interests. Yet Burke was, in fact, a great champion of reform in his day—and the leading defender of the American colonists' grievances against British oppression before the Revolution. "A State without the means of some change is without the means of its conservation," Burke wrote.[42]

The same is true of the Internet ecosystem when it comes to improving data collection practices and user empowerment: Ultimately, we *do* need better user empowerment tools like "Do Not Track." Yet there is a middle ground between doing nothing and the insistence of those privacy Jacobins who demand immediate, sweeping intervention, no matter its costs, because privacy is a "fundamental right" that must be protected at any cost—"*Fiat justitia ruat coelom*," as Latin-loving lawyers say: "May justice be done though the heavens fall."

The FTC has a key role to play in this process, as Commissioner Rosch has argued. Yet "Rome was not built in a day," and neither will be a sustainable privacy marketplace that works for both consumers and publishers, as well as the advertisers and ad networks who "keep the party going" for everyone. Where the market process of discovery through innovation is working, government should not interfere. That process is well underway with "Do Not Track." There is much to lose by rushing forward. The FTC should follow Burke's maxim: "Our patience will achieve more than our force."[43] Participating in the inter-agency working process outlined by the Department of Commerce in its Green Paper will be a good way for the FTC to put its "patience" to good use—helping to improve best practices, but not dictating them.

---

41 *See generally* VIRGINIA POSTREL, THE FUTURE AND ITS ENEMIES (1998).

42 Edmund Burke, Reflections on the Revolution in France (1790), available at http://www.constitution.org/eb/rev_fran.htm.

43 *Id.*

Harvard Journal of Law & Technology
Volume 25, Number 1 Fall 2011

TRAGEDY OF THE DATA COMMONS

*Jane Yakowitz**

TABLE OF CONTENTS

---

* Visiting Assistant Professor of Law, Brooklyn Law School; Yale Law School, J.D.; Yale College, B.S. The author is grateful for invaluable feedback from Jeremy Albright, Jonathan Askin, Miriam Baer, Derek Bambauer, Daniel Barth-Jones, Anita Bernstein, Frederic Bloom, Ryan Calo, Deven Desai, Robin Effron, Khaled El Emam, Marsha Garrison, Robert Gellman, Eric Goldman, Dan Hunter, Ted Janger, Margo Kaplan, Claire Kelly, Bailey Kuklin, Rebecca Kysar, Brian Lee, David S. Levine, Andrea M. Matwyshyn, Bill McGeveran, Helen Nissenbaum, Paul Ohm, Richard Sander, Liz Schneider, Paul Schwartz, Christopher Soghoian, Larry Solan, Berin Szoka, Nelson Tebbe, Adam Thierer, Marketa Trimble, Felix Wu, and Peter Yu. This article was generously supported by the Brooklyn Law School Dean's Summer Research Stipend Program.

I. INTRODUCTION

Over the past ten years, the debate over welfare reform has been transformed by Jeffrey Grogger and his coauthors. Grogger's data-driven research shows, among other things, that work requirements and time limits may have no effect on marriage or fertility rates.[1] In other words, welfare does not produce "welfare queens." More recently, Roland Fryer and Steven Levitt have discredited Herrnstein's theory that the test score gap between Caucasians and African Americans is the result of biological differences. Fryer and Levitt used longitudinal data to document for the first time that there are no differences in the cognitive skills of white and black nine-month-old babies, and that the gap that develops by elementary school is explained almost entirely by socio-economic and environmental factors.[2] And in 2001, John J. Donohue and Steven D. Levitt presented shocking evidence that the decline in crime rates during the 1990s, which had defied explanation for many years, was caused in large measure by the introduction of legalized abortion a generation earlier.[3]

These studies and many others have made invaluable contributions to public discourse and policy debates, and they would not have been possible without anonymized research data — what I call the "data commons." The data commons is comprised of the disparate and

1. JEFFREY GROGGER & LYNN A. KAROLY, WELFARE REFORM: EFFECTS OF A DECADE OF CHANGE 196–97 (2005). Grogger has also produced empirical evidence that welfare-to-work reforms did lead to increased wages and increased rates of non-dependence among the welfare recipients, but also had a negative impact on the academic performance of their adolescent children. Jeff Grogger & Charles Michalopoulos, *Welfare Dynamics Under Term Limits* (Nat'l Bureau of Econ. Research, Working Paper No. 7353, 1999); Jeffrey Grogger, Lynn A. Karoly & Jacob Alex Klerman, *Conflicting Benefits Trade-Offs in Welfare Reform*, RAND.ORG (2002), http://www.rand.org/publications/randreview/issues/rr-12-02/benefits.html.

2. Roland G. Fryer, Jr. & Steven D. Levitt, *Understanding the Black-White Test Score Gap in the First Two Years of School*, 86 REV. ECON. & STAT. 447, 447 (2004); Roland G. Fryer, Jr. & Steven D. Levitt, *Testing for Racial Differences in the Mental Ability of Young Children* (Nat'l Bureau of Econ. Research, Working Paper No. 12066, 2006).

3. John J. Donohue III & Steven D. Levitt, *The Impact of Legalized Abortion on Crime*, 116 Q.J. ECON. 379 (2001).

diffuse collections of data made broadly available to researchers with only minimal barriers to entry. We are all in the data commons; information from our tax returns, medical records, and standardized tests seed the pastures. We are protected from embarrassment and misuse by anonymization. But a confluence of events has motivated privacy experts to abandon their faith in data anonymization.

In his recent article, Paul Ohm brought the concerns of the computer science community to a wide audience of lawyers and policymakers. Ohm's argument is simple and superficially sound: As the amount of publicly available information on the Internet grows, so too does the chance that a malfeasor can reverse engineer a dataset that was once anonymized and expose sensitive information about one of the data subjects.[4] Privacy advocates, the media, and the Federal Trade Commission ("FTC") have accepted uncritically the notion that anonymization is impossible, and they advocate for the wholesale dismantling of the concept of anonymization.[5] In its place, privacy advocates recommend that research data should be regulated under the strong property and autonomy models of privacy favored by Lawrence Lessig, Jerry Kang, Paul Schwartz, and other scholars.[6]

Today, data privacy practices are shaped by some combination of ambiguous statutory directives, inconsistent case law, industry best practices, whim, and self-serving discretionary preferences. The time is ripe for the creation of uniform data privacy policies, and there is much to fix.[7] But proposals that inhibit the dissemination of research data dispose of an important public resource without reducing the pri-

---

4. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

5. *See id. See generally* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010) [hereinafter FTC PRIVACY REPORT], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; Ryan Singel, *Netflix Spilled Your* Brokeback Mountain *Secret, Lawsuit Claims*, WIRED THREAT LEVEL (Dec. 17, 2009, 4:29 PM), http://www.wired.com/threatlevel/2009/12/netflix-privacy-lawsuit; Seth Schoen, *What Information is "Personally Identifiable"?*, ELECTRONIC FRONTIER FOUND. DEEPLINKS (Sept. 11, 2009, 10:43 PM), http://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable; *Re-identification*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/reidentification/ (last visited Dec. 21, 2011). Parties in several recent lawsuits have argued that there is no longer a tenable difference between anonymized information and personally identifiable information. *See, e.g.*, Complaint at 20, Gaos v. Google Inc., No. 10-CV-04809 (N.D. Cal. May 2, 2011); Complaint at 15, Doe v. Netflix, No. C09 05903 (N.D. Cal. Dec. 17, 2009) [hereinafter Doe Complaint]; Elinor Mills, *AOL Sued over Web Search Data Release*, CNET NEWS BLOGS (Sept. 25, 2006, 12:17 PM), http://news.cnet.com/8301-10784_3-6119218-7.html.

6. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 142–63 (1999); Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 229, 255 (2004); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2076, 2088–113 (2004).

7. Privacy law is on the mind of politicians and regulators and has entered what John Kingdon calls the proverbial "policy window." JOHN KINGDON, AGENDAS, ALTERNATIVES, AND PUBLIC POLICIES 165 (2d ed. 2002).

vacy risks that actually put us in peril. This Article argues that it is in fact the research data that is now in great need of protection. People have begun to defensively guard anonymized information about themselves. We are witnessing a modern example of a tragedy of the commons.[8] Each individual has an incentive to remove her data from the commons to avoid remote risks of re-identification. This way she gets the best of both worlds: her data is safe, and she also receives the indirect benefits of helpful health and policy research performed on the rest of the data left in the commons. However, the collective benefits derived from the data commons will rapidly degenerate if data subjects opt out to protect themselves.[9]

This Article challenges the dominant perception about the risks of research data by making three core claims. First, the social utility of the data commons is misunderstood and greatly undervalued by most privacy scholars. Public research data produces rich contributions to our collective pursuit of knowledge and justice. Second, the influential legal scholarship by Ohm and others misinterprets the computer science literature, and as a result, oversells the futility of anonymization, even with respect to theoretical risk. And third, the realistic risks posed by the data commons are negligible. So far, there have been no known occurrences of improper re-identification of a research dataset. Even the hypothetical risks are smaller than other information-based risks (from data spills or hacking, e.g.) that we routinely tolerate for convenience.

The Article proceeds as follows: Parts II, III, and IV perform a risk-utility calculus on the data commons, finding that the public data commons is tremendously valuable (Part II), that the theoretical risks of research data are exaggerated (Part III), and that the true risks posed by research data are nonexistent (Part IV). Together, Parts II

---

8. The tragedy of the commons model I explore here is not perfectly analogous to the "grazing commons" concept popularized by Garrett Hardin. Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968). In the grazing model, self-interested actors convert the communal benefits of the commons into private benefits for themselves. The gain from adding one more cow of their own is internalized, while the losses in the form of overgrazing are externalized and borne by the entire population. *Id.* In the data commons, the data subject depletes the commons by removing his data. The marginal detriment of his decision is externalized and shared across the entire population. Meanwhile, he enjoys the full value of the avoided risk of re-identification. Unlike the traditional commons examples, each actor is constrained in how much of the commons he is capable of depleting since he has but one line of data to remove. (The grazing and pollution examples that Hardin discusses anticipate actors who deposit multiple cows, or increasing amounts of pollution, into the commons). But the key point is intact: communal benefits are lost due to actions motivated by self-interest. Vaccination makes an even better comparison. *See infra* Part VI.

9. Fred Cate makes a similar argument in the context of consumer data used for credit reports. *See* Fred H. Cate, Data and Democracy, Herman B Wells Distinguished Lecture of the Institute and Society for Advanced Study (Sept. 21, 2001), *in* IND. UNIV., INST. FOR ADVANCED STUDY AND SOC'Y FOR ADVANCED STUDY, HERMAN B WELLS DISTINGUISHED LECTURE SERIES 1 (2001), *available at* https://scholarworks.iu.edu/dspace/bitstream/handle/2022/8508/IAS-WDLS-01.pdf.

through IV show that concerns over anonymized data have all the characteristics of a moral panic and are out of proportion to the actual threat posed by data dissemination.[10] In Part V, I put forward a bold proposal to redesign privacy policy such that public research data would be *easier* to disseminate. While data users who intentionally re-identify a subject in an anonymized dataset should be sanctioned heavily, agencies and firms that compile and produce the data in the commons should receive immunity from statutory or common law privacy claims so long as they undergo basic anonymization techniques. Part V also provides clear guidance for data producers operating under the current statutory regime. Part VI concludes with an appeal to the legal community to think and talk about research data differently. The bulk of privacy scholarship has had the deleterious effect of exacerbating public distrust in research data. Rather than encouraging the public to fervently guard their self-interest, scholars should build a sense of civic responsibility to pay their "information taxes" and participate in research datasets.

II. FRUITS OF THE DATA COMMONS

The benefits flowing from the data commons are indirect but bountiful. Thus far, the nascent technical literature on de-anonymization has virtually ignored the opportunity costs that would result from a drastic reduction in data sharing.[11] Legal scholars who write on the topic acknowledge the public interest in information, but they give that interest short shrift and describe it in abstract terms.[12]

---

10. For a discussion of "moral panics," see STANLEY COHEN, FOLK DEVILS AND MORAL PANICS (1972). Here, advocacy groups' demand for political action is driven by fears that privacy and anonymity as we know them are on the brink of ruin.

11. For example, the Netflix de-anonymization study, on which Ohm relies heavily, makes no effort to compare the risk of re-identification to the utility of the dataset. Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, 2008 PROC. 29TH IEEE SYMP. ON SECURITY & PRIVACY 111. The early work of Latanya Sweeney acknowledged a tradeoff between a dataset's utility and its theoretical re-identification risk, but the discussion of utility was abstract and very brief. Moreover, Sweeney's recent work pays no regard to the countervailing interests in data utility at all. *Compare* Latanya Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection (May 2001) (unpublished Ph.D. thesis, Massachusetts Institute of Technology), *available at* http://dspace.mit.edu/bitstream/handle/1721.1/8589/49279409.pdf, *with* Latanya Sweeney, *Patient Identifiability in Pharmaceutical Marketing Data* (Data Privacy Lab Working Paper 1015, 2011), *available at* http://dataprivacylab.org/projects/identifiability/pharma1.pdf. The statistical literature on disclosure risk generally recognizes the tension between the utility of data sharing and its concomitant risks but struggles to define best practices that can persist with increasing amounts of data accumulation. For a review of the state of the current computer science literature on the subject, see GEORGE T. DUNCAN ET AL., STATISTICAL CONFIDENTIALITY: PRINCIPLES AND PRACTICE (2011).

12. *See, e.g.*, PAUL M. SCHWARTZ, THE CTR. FOR INFO. POLICY LEADERSHIP, DATA PROTECTION LAW AND THE ETHICAL USE OF ANALYTICS 8 (2010), *available at* http://www.huntonfiles.com/files/webupload/CIPL_Ethical_Undperinnings_of_Analytics_Paper.pdf; Ohm, *supra* note 4, at 1708, 1714. *But see, e.g.*, Douglas J. Sylvester & Sharon

To strike the right balance between the public's interest in privacy and its interest in the data commons, we must have a more concrete understanding of the value gleaned from broadly accessible research data. In this Part, I define the data commons and explore its utility. I also discuss government agencies' pretextual use of privacy law to evade Freedom of Information Act ("FOIA") requests when disclosures could reveal something embarrassing to the government.

A. Research Data

This Article addresses datasets that are compiled and shared broadly for "research," by which I mean a methodical study designed to contribute to human knowledge by reaching verifiable and generalizable conclusions.[13] Although this is an expansive definition of "research," it importantly excludes analytic studies on the subject pool for the purpose of understanding the particular individuals in the pool, as opposed to understanding a general population.[14]

Public-use research datasets are usually subject to legal constraints that guard the privacy of the data subjects, and the largest producers of research data (including the U.S. Census Bureau and other federal agencies) use sophisticated anonymization techniques that go well beyond the minimum legal requirements.[15] Privacy laws in their various forms usually prohibit the release of personally identifiable

---

Lohr, *The Security of Our Secrets: A History of Privacy and Confidentiality in Law and Statistical Practice*, 83 DENV. U. L. REV. 147, 196–99 (2005); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1122–24 (2000).

13. 45 C.F.R. § 164.501 (2010) (defining research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge").

14. A business entity might be very interested in what the particular individuals in its, or a competitor's, databases are like and inclined to purchase, regardless of whether their analytics can be generalized to describe human phenomena. Data researchers are naturally indifferent to information about any particular person because information about that person cannot be generalized to any class of persons. "Statistical data are unconcerned with individual identities. They are collected to answer questions such as 'how many?' or 'what proportion?', not 'who?'. The identities and records of co-operating (or non-cooperating [sic]) subjects should therefore be kept confidential, whether or not confidentiality has been explicitly pledged." *ISI Declaration on Professional Ethics*, INT'L STAT. INST. (Aug. 1985), http://isi-web.org/about/ethics1985; *see also* Sylvester & Lohr, *supra* note 12, at 185.

15. *See*, *e.g.*, *Confidentiality Statement*, U.S. CENSUS BUREAU, http://factfinder.census.gov/jsp/saff/SAFFInfo.jsp?_pageId=su5_confidentiality (last updated Mar. 17, 2009). These techniques include top-coding, data swapping, and the addition of random noise. *See* Jerome P. Reiter, *Estimating Risks of Identification Disclosure in Microdata*, 100 J. AM. STAT. ASS'N 1103, 1103 (2005). While these techniques increase privacy, they come at a cost to the utility of the data since the fuzzied data affects the results of statistical analyses. *See, e.g.*, A. F. Karr et al., *A Framework for Evaluating the Utility of Data Altered to Protect Confidentiality*, 60 AM. STATISTICIAN 224, 224 (2006). Data archivists and social scientists conceive of privacy obligations differently from lawmakers and, not surprisingly, their approach is more nuanced.

information ("PII").[16] Information is personally identifiable if it can be traced to a specific individual.[17] Obviously, information that is tied to a direct identifier, such as name, address, or social security number, is personally identifiable. For example:

> Jane Yakowitz is actually a giant cockroach.

However, PII is not limited to information that directly identifies a subject. Included in its ambit are pieces of information that can be used in combination to indirectly link sensitive information to a particular person.

> A 31-year-old white female who works at Brooklyn Law School and lives in ZIP code 11215 is actually a giant cockroach.

Or:

> All 31-year-old females that live in ZIP code 11215 are actually giant cockroaches.

I will use the term "indirect identifiers" to mean pieces of information that can lead to the identity of a person through cross-reference to other public sources or through general knowledge.[18] "Non-identifiers," in contrast, cannot be traced to individuals without having special non-public information.

Paul Ohm has criticized U.S. privacy law for using static definitions of what constitutes PII,[19] but his description of the law is inaccu-

---

16. See discussion of the Family Education Rights and Privacy Act ("FERPA"), Health Insurance Portability and Accountability Act ("HIPAA"), and the Confidential Information Protection and Statistical Efficiency Act *infra* text accompanying notes 20–21.

17. For example, the HIPAA Standards for Privacy of Individually Identifiable Health Information (the "HIPAA Privacy Rule") define individually identifiable information as information that "identifies the individual" or information "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103 (2010).

18. I borrow this term from the Department of Education's commentary on the final ruling of the 2008 revisions to the FERPA regulations. Family Educational Rights and Privacy, 73 Fed. Reg. 74,806, 74,831 (Dec. 9, 2008). Although some use other terminology such as "high risk variables," I prefer the term "indirect identifier" because it connotes that the information might be usable for tracing an identity without implying that it always and necessarily heightens the risk of re-identification to an unacceptable level. Latanya Sweeney, the computer scientist at Carnegie Mellon University who popularized the k-anonymity model for de-identifying data, uses the term "quasi-identifiers." Latanya Sweeney, *k-Anonymity: A Model for Protecting Privacy*, 10 INT'L J. UNCERTAINTY, FUZZINESS AND KNOWLEDGE-BASED SYSTEMS 557, 563 (2002).

19. Ohm, *supra* note 4, at 1740–41. Paul Ohm suggests modifying the rhetoric used in information privacy to connote that common privacy techniques merely "try to achieve anonymity," and do not actually achieve it. *Id.* at 1744. I like his recommendation to use the

rate. Privacy statutes list categories of information that necessarily must be classified as indirect identifiers (such as sex and ZIP code), but the statutes also obligate data producers to guard against other unspecified indirect identifiers that, in context, could be used to re-identify a subject. For example, the Confidential Information Protection and Statistical Efficiency Act ("CIPSEA") disallows the disclosure of statistical data or information that is in "identifiable form," defined as "any representation of information that permits the identity of the respondent to whom the information applies to be reasonably inferred by either direct or indirect means."[20] The Family Education Rights and Privacy Act ("FERPA") and the regulations implemented under the Health Insurance Portability and Accountability Act ("HIPAA") define PII similarly, with savings clauses that prohibit releases that might be reverse engineered through indirect means.[21]

The PII standard has a significant impact on the data commons. Large, information-rich datasets will inevitably contain PII because the combinations of indirect identifiers are likely to make some of the subjects unique, or close to it. Thus, even the legal minimum anonymization requires some of the utility of a dataset to be lost through redaction and blurring in order to ensure that no subject has a unique combination of indirect identifiers.

B. The Value of the Data Commons

In 1997, policy researchers at the RAND Corporation warned that the Sentencing Reform Act of 1984 and the plethora of state statutes setting minimum sentencing requirements for drug convictions are a less cost-effective means to reduce the consumption of cocaine than

---

term "scrub," *id.*, but Ohm's linguistic analysis reveals something about his assumptions. To Ohm, there never *was* a difference between *trying to achieve* anonymity and anonymity; anonymization techniques were never believed to be completely without risk.

20. E-Government Act of 2002, Pub. L. No. 107-347, § 502(4), 116 Stat. 2962, 2962 (codified at 44 U.S.C. § 3501 note).

21. *See* FERPA, 20 U.S.C.A. § 1232g (West 2010 & Supp. 2011); HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160.103 (2010). Usually, multiple indirect identifiers have to be combined in order to ascertain the identity of a specific individual. Privacy law is mindful of this potential route to re-identification and explicitly guards against it — any combination of publicly knowable information that can be used to trace to an identity is PII. The FERPA regulations prohibit the disclosure of "[o]ther information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty." 34 C.F.R. § 99.3 (2010). The HIPAA Privacy Rule prohibits the disclosure of "protected health information," 45 C.F.R. § 164.502 (2010), including information "(i) [t]hat identifies the individual; or (ii) [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." *Id.* § 160.103.

the previous system.[22] Moreover, both enforcement regimes were less effective per dollar spent on enforcement than on treatment programs.[23] While the change in policy could be defended on the basis of retributive goals, the promised deterrent effects were illusory.[24] Now that states are facing gaping budget holes, the tune has changed. The severity and consistency of drug convictions are no longer political imperatives, and the costs of maintaining prisons are causing consternation.[25] Voters in Arizona and California passed legislation to reduce sentencing for low-level drug offenders.[26] This may seem like sound policy, given the tenuous relationship between sentencing time and deterrence, but a new study produced by RAND shows that this policy move might be ill advised, too.[27] During the last twenty years, prosecutors have altered their behavior to adapt to the minimum sentencing laws by using them as bargaining power to secure plea bargains.[28] As a result, offenders serving prison time today for low-level drug offenses usually have much more serious criminal histories than their records suggest.[29] Both of the RAND studies have made important contributions to the complex debate on crime and drug policy, and both were made possible by the data commons.[30]

If data anonymity is presumed not to exist, the future of public-use datasets and all of the social utility flowing from them will be thrown into question. Nearly every recent public policy debate has benefited from mass dissemination of anonymized data. Public use data released by the Federal Financial Institutions Examination Council provides a means of detecting housing discrimination and informs

22. JONATHAN P. CAULKINS ET AL., RAND, MANDATORY MINIMUM DRUG SENTENCES: THROWING AWAY THE KEY OR THE TAXPAYERS' MONEY? 62 (1997), *available at* http://www.rand.org/pubs/monograph_reports/MR827.html.

23. *Id.*

24. U.S. SENTENCING COMM'N, SPECIAL REPORT TO THE CONGRESS: MANDATORY MINIMUM PENALTIES IN THE FEDERAL CRIMINAL JUSTICE SYSTEM iii (1991) ("Deterrence, a primary goal of the Sentencing Reform Act and the Comprehensive Crime Control Act, is dependent on certainty and appropriate severity.").

25. K. JACK RILEY ET AL., RAND, JUST CAUSE OR JUST BECAUSE?: PROSECUTION AND PLEA-BARGAINING RESULTING IN PRISON SENTENCES ON LOW-LEVEL DRUG CHARGES IN CALIFORNIA AND ARIZONA xiii (2005), *available at* http://www.rand.org/pubs/monographs/MG288.html.

26. Substance Abuse and Crime Prevention Act of 2000, Cal. Prop. 36 (codified at CAL. PENAL CODE § 1210 (West 2006)); Act Relating to Laws on Controlled Substances and those Convicted of Personal Use or Possession of Controlled Substances, Prop. 200, (Ariz. 1996) (codified as amended at ARIZ. REV. STAT. ANN. § 41–1404.16 (2011).

27. RILEY ET AL., *supra* note 25, at 76.

28. *Id.* at 62.

29. *Id.* at 76.

30. The 1997 study used data from the U.S. Drug Enforcement Agency's System to Retrieve Information from Drug Evidence ("STRIDE") and from the National Household Survey on Drug Abuse. CAULKINS, *supra* note 22, at 85. The 2005 study used data from the California and Arizona Departments of Corrections. RILEY ET AL., *supra* note 25, at 20, 24.

policy debates over the home mortgage crisis.[31] Research performed by health economists and epidemiologists using Medicare and Medicaid data is now central to the debates about health care reform.[32] Census microdata has been used to detect racial segregation trends in housing.[33] Public-use birth data has led to great advances in our understanding of the effects of smoking on fetuses.[34] Public crime data has been used to reveal the inequitable allocation of police resources based on the socio-economic status of neighborhoods.[35] And the data commons is repeatedly used to expose fraud and discrimination that would not be discoverable or provable based on the experience of a single person.[36]

None of this data would be available to the broad research community under a conception of privacy that abandons hope in anonymization. These datasets are critical to what George T. Duncan calls "Information Justice," which is the fairness that accessible information offers to the general public in the form of knowledge, and offers to individuals in the form of a discoverable and verifiable grievance.[37]

C. Ex Ante Valuation Problems

The value of a research database is very difficult to discern in the abstract, before researchers have had a chance to analyze it. The uncertain value makes it difficult to know when privacy interests ought to succumb to the public interest in data sharing. Paul Schwartz demonstrates the problem when he argues that some types of information do not implicate data privacy: "[S]ome kinds of aggregate in-

---

31. Press Release, Federal Financial Institutions Examination Council (Sept. 8, 2006), *available at* http://www.ffiec.gov/hmcrpr/hm090806.htm; Janneke Ratcliffe & Kevin Park, Written Comments and Supplement to Oral Testimony Provided by Janneke Ratcliffe at the Hearing on Community Reinvestment Act Regulations (Aug. 31, 2010), *available at* http://www.ccc.unc.edu/documents/CRA_written_8.6.2010.v2.pdf.

32. *See, e.g.*, Jacob S. Hacker, Inst. for America's Future, *Public Plan Choice in Congressional Health Plans*, CAMPAIGN FOR AMERICA'S FUTURE (Aug. 20, 2009), http://www.ourfuture.org/files/Hacker_Public_Plan_August_2009.pdf.

33. Casey J. Dawkins, *Recent Evidence on the Continuing Causes of Black-White Residential Segregation*, 26 J. URB. AFF. 379, 379 (2004).

34. Allen J. Wilcox, *Birth Weight and Perinatal Mortality: The Effect of Maternal Smoking*, 137 AM. J. EPIDEMIOLOGY 1098, 1098 (1993).

35. Cate, *supra* note 9, at 14.

36. For example, the data routinely collected by the Equal Employment Opportunity Commission is used to check for statistically significant disparities between racial and gender groups. *See, e.g.*, Paul Meier, Jerome Sacks & Sandy L. Zabell, *What Happened in* Hazelwood*: Statistics, Employment Discrimination, and the 80% Rule*, 1984 AM. B. FOUND. RES. J. 139.

37. George T. Duncan, *Exploring the Tension Between Privacy and the Social Benefits of Governmental Databases*, *in* A LITTLE KNOWLEDGE: PRIVACY, SECURITY AND PUBLIC INFORMATION AFTER SEPTEMBER 71, 82 (2004) (Peter M. Shane, John Podesta & Richard C. Leone eds., Century Foundation 2004).

formation involve pools that are large enough to be viewed, at the end of the day, as purely statistical and thus, as raising scant privacy risks as a functional matter."[38] He cites flu trends as an illustration of this sort of aggregate non-problematic data.[39] But Google's Flu Trends — the fastest and most geographically accurate way to monitor national flu symptoms[40] — only works by collecting *all* Google search queries by IP address.[41] This practice runs afoul of Schwartz's admonition against collecting information without a specific and limited purpose.[42]

Google Flu Trends exemplifies why it is not possible to come to an objective, prospective agreement on when data collection is sufficiently in the public's interest and when it is not.[43] Flu Trends is an innovative use of data that was not originally intended to serve an epidemiological purpose. The program uses data that, in other contexts, privacy advocates believe violates Fair Information Practices.[44] This illustrates a concept understood by social scientists that is frequently discounted by the legal academy and policy-makers: some of the most useful, illuminating data was originally collected for a completely unrelated purpose. Policymakers will not be able to determine in advance which data resources will support the best research and make the greatest contributions to society. To assess the value of research data, we cannot cherry-pick between "good" and "bad" data collection.[45]

Take another example, recently reproduced in the Freakonomics blog. The online dating website OkCupid analyzes all of the information entered by its members to reveal interesting truths about the

---

38. SCHWARTZ, *supra* note 12, at 8.

39. *Id.* at 8, 15.

40. Miguel Helft, *Aches, a Sneeze, a Google Search*, N.Y. TIMES, Nov. 12, 2008, at A1.

41. Miguel Helft, *Is There a Privacy Risk in Google Flu Trends?*, N.Y. TIMES BITS (Nov. 13, 2008, 8:20 PM), http://bits.blogs.nytimes.com/2008/11/13/does-google-flu-trends-raises-new-privacy-risks.

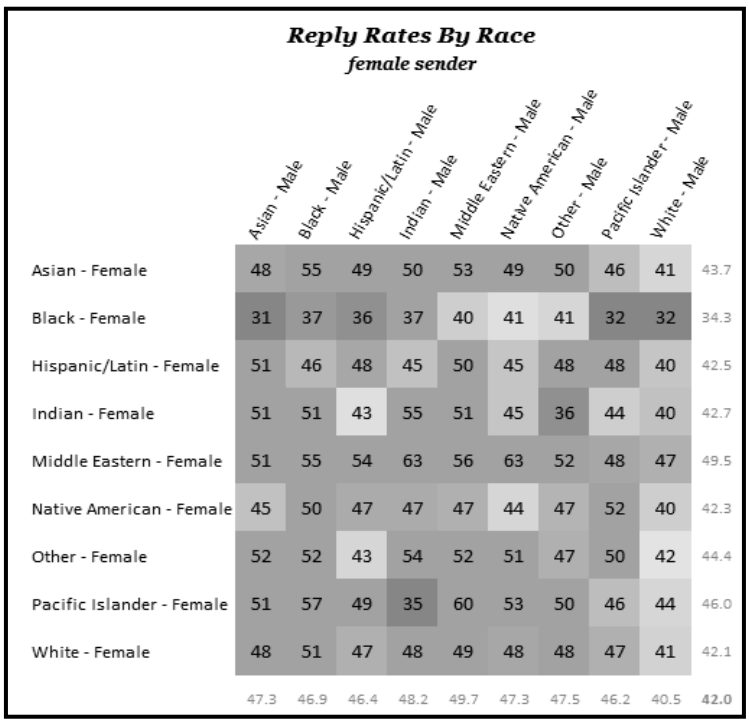
42. SCHWARTZ, *supra* note 12, at 24.

43. The problem of valuing information is as old as privacy. Samuel Warren and Louis Brandeis believed that the press in their day was overstepping "the obvious bounds of propriety and of decency" by photographing the private lives of public and elite figures for the gossip pages. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890). But today gossip journalism is imbedded into mainstream culture and often the spearhead for the uncovering of important news items. *See* David Perel, *How the Enquirer Exposed the John Edwards Affair*, WALL ST. J., Jan. 23, 2010, at A15.

44. *Google Watches as You Type in Search Words and Displays "Live" Results in Real Rime. Creeped Out, So Are We*., TECHALOUD (Aug. 23, 2010), http://www.techaloud.com/2010/08/google-tests-search-results-that-update-as-you-type (expressing displeasure with Google's use of private information in generating search terms); Chris Jay Hoofnagle, *Beyond Google and Evil: How Policy Makers, Journalists and Consumers Should Talk Differently About Google and Privacy*, FIRST MONDAY (Apr. 6, 2009), http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2326/2156.

45. *But see* Roger Clarke, *Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism*, 4 INFO. INFRASTRUCTURE & POL'Y 29 (1995).

dating public.[46] In one fascinating study, the OkCupid researchers found that men of all races responded to the initial contacts of black females at significantly lower rates, despite the fact that the profiles of black females are as compatible as the females of every other race.[47]



Reply Rates By Race

female sender

	Asian - Male	Black - Male	Hispanic/Latin - Male	Indian - Male	Middle Eastern - Male	Native American - Male	Other - Male	Pacific Islander - Male	White - Male	
Asian - Female	48	55	49	50	53	49	50	46	41	43.7
Black - Female	31	37	36	37	40	41	41	32	32	34.3
Hispanic/Latin - Female	51	46	48	45	50	45	48	48	40	42.5
Indian - Female	51	51	43	55	51	45	36	44	40	42.7
Middle Eastern - Female	51	55	54	63	56	63	52	48	47	49.5
Native American - Female	45	50	47	47	47	44	47	52	40	42.3
Other - Female	52	52	43	54	52	51	47	50	42	44.4
Pacific Islander - Female	51	57	49	35	60	53	50	46	44	46.0
White - Female	48	51	47	48	49	48	48	47	41	42.1
	47.3	46.9	46.4	48.2	49.7	47.3	47.5	46.2	40.5	**42.0**

Figure 1: OkCupid Analysis of Member Messaging Behavior[48]

One of the most remarkable aspects of the OkCupid study is that it did not draw the ire of privacy advocates.[49] Contrast Freakonomics's coverage of the OkCupid study with the *L.A. Times*'s coverage of a Facebook study that came to the unsurprising conclusion that Facebook statuses are cheery on holidays and dreary when celebrities die: "If you put something on Facebook, no matter how tight your privacy settings are, Facebook Inc. can still hang onto it, analyze it,

46. *See* Ian Ayres, *Race and Romance: An Uneven Playing Field for Black Women*, FREAKONOMICS, (Mar. 3, 2010, 2:00 PM), http://www.freakonomics.com/2010/03/03/race-and-romance-an-uneven-playing-field-for-black-women.

47. *Id.*

48. *Id.*

49. Its own privacy assurances seemed to have deflected criticism well enough. *See* Jason Del Rey, *In Love with Numbers: Getting the Most out of Your Company Data*, INC. MAGAZINE, Oct. 2010, at 105, 106.

remix it and repackage it. Despite its silly name, the Gross National Happiness indicator is creepy. *We're* in there."[50]

How is it that Facebook's study attracted criticism of its privacy policies while the data used in the OkCupid study went unnoticed? The difference is likely explained by the value of the OkCupid study. The OkCupid study's contribution to our understanding of human relations distracts commentators from thinking about the source of the data. The utility of the research overshadows our collective anxiety about research data. The trouble is that the public and the press undervalue the beneficial uses of research data when the attention turns to data privacy.

The OkCupid study illustrates another important quality of research microdata: that collectively, our data reveals more than any of us could know on our own. The message-writing decisions of each individual OkCupid member could not have revealed the patterns of preferences, but when aggregated, the data supports a hypothesis about human nature and implicit bias. Research data describes everybody without describing anybody. If the data from the OkCupid profiles was thought to be the property of the members, subject to their exclusive determination on the uses to which it is put, society at large, and OkCupid members in particular, would be deprived of the discovery of this quiet pattern.

D. The Importance of Broad Accessibility

The value of data is not completely lost on privacy law scholars, but the need for broad access generally is. When data can be shared freely, it creates a research dialog that cannot be imitated through restricted data and license agreements. In contrast to legal scholars, technology journalists recognize the unmatchable virtues that come from crowdsourcing when all interested people have unfettered access to data.[51] General access ensures the best chance that a novel or creative use of a dataset will not be missed.

Privacy laws that constrain the dissemination of the most useful data through discretionary licensing agreements (such as HIPAA and FERPA) are designed without sufficient appreciation as to how research works. Ironically, they operate on a model that gives researchers too much credit, and has too much faith that data supports just one unassailable version of the truth. In practice, transparency and data sharing are integral to a researcher's credibility. The data commons

50. Mark Milian, *Facebook Digs Through User Data and Graphs U.S. Happiness*, L.A. TIMES TECH. (Oct. 6, 2009, 3:50 PM), http://latimesblogs.latimes.com/technology/2009/10/facebook-happiness.html.

51. *See, e.g.*, *Of Governments and Geeks*, ECONOMIST, Feb. 6, 2010, at 65; Chris Soghoian, *AOL, Netflix and the End of Open Access to Research Data*, CNET SURVEILLANCE STATE (Nov. 30, 2007, 8:30 AM), http://news.cnet.com/8301-13739_3-9826608-46.html.

protects the public discourse from two common research hazards: (1) the failure to catch innocent mistakes, which are legion, and (2) the restriction of access to highly useful data based on ideological considerations or self-interest.

Replication is indispensable to the process of achieving credible, long-lasting results.[52] Just as mistakes and even fabrications occur in the hard sciences,[53] they also occur in the social sciences. The gatekeepers at peer-reviewed science and economics journals have proven to be significantly less effective than the motivated monitoring of peers and foes in the field.[54] For example, a study published in England's preeminent health research journal claimed to have found statistical proof that women can increase the chance of conceiving a male fetus if they eat breakfast cereal.[55] The findings were covered by the *New York Times* and National Public Radio.[56] When the data was made available to other researchers, the results quickly fell apart and have become something of a cautionary tale against researchers that torture a dataset into producing statistically significant results.[57] Simple coding errors are even more common and can distort and completely invert results. Because of the frequency and inevitability of these sorts of errors, the most respected journals make data sharing a prerequisite for publication (and even article submission).[58]

Consider the debate on the deterrent effects of the death penalty. In 1972, the U.S. Supreme Court determined that existing death penalty statutes and practices violated convicts' Eighth Amendment right to

---

52. *See* Gary King, *Replication, Replication*, 28 PS: POL. SCI. & POLITICS 444, 444 (1995).

53. *See Spectacular Fraud Shakes Stem Cell Field*, MSNBC (Dec. 23, 2005), http://www.msnbc.msn.com/id/10589085/ns/technology_and_science-science.

54. The National Institute of Health found that only one out of every twenty claims flowing from observational studies ends up being reproducible in controlled studies. S. Stanley Young, *Everything Is Dangerous: A Controversy*, AM. SCIENTIST (Apr. 22, 2009), http://www.americanscientist.org/science/pub/everything-is-dangerous-a-controversy.

55. Fiona Mathews, et al., *You Are What Your Mother Eats: Evidence for Maternal Preconception Diet Influencing Foetal Sex in Humans*, 275 PROC. ROYAL SOC'Y B 1661, 1665 (2008).

56. Tara Parker-Pope, *Boy or Girl? The Answer May Depend on Mom's Eating Habits*, N.Y. TIMES WELL (April 23, 2008, 12:59 PM), http://well.blogs.nytimes.com/2008/04/23/boy-or-girl-the-answer-may-depend-on-moms-eating-habits; Allison Aubrey, *Can a Pregnant Woman's Diet Affect Baby's Sex?*, (NPR radio broadcast Jan. 15, 2009), *available at* http://www.npr.org/templates/story/story.php?storyId=99346281.

57. *See* Young, *supra* note 54.

58. NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, SHARING PUBLICATION-RELATED DATA AND MATERIALS: RESPONSIBILITIES OF AUTHORSHIP IN THE LIFE SCIENCES 3 (2003). *Science*, an academic journal, changed its review policy in 2006 to require all authors to post the raw data supporting their findings online after the discovery that one of the most important stem cell research findings at that time was a complete fabrication. *See* Barry R. Masters, Book Review, 12 J. BIOMEDICAL OPTICS 039901-1, 039901-1 (2007) (reviewing ADIL E. SHAMOO & DAVID B. RESNIK, RESPONSIBLE CONDUCT OF RESEARCH (2003)).

be free from cruel and unusual punishment.[59] But three years later, an explosive empirical study by Isaac Ehrlich concluded that each execution had the effect of saving up to eight lives by deterring would-be criminals from killing.[60] Robert Bork, then the Solicitor General, cited to Ehrlich's study in his brief for *Gregg v. Georgia*[61] a year later and, lo and behold, the Supreme Court was persuaded to end the moratorium on death sentences.[62] The trouble is, Ehrlich's persuasive study has not stood the test of time and replication. Since then, the capital punishment debate has attracted the attention of many prized economists.[63] John J. Donohue and Justin Wolfers have shown that the empirical studies finding a deterrent effect are highly sensitive to the choice of sampling periods and other discretionary decisions made by the studies' authors.[64] The deterrent effects found by Ehrlich are in doubt, now that economists have had the opportunity to test the robustness of the findings and explore the idiosyncratic series of methodological decisions that led to them.[65] Had Ehrlich alone had access to the crime data supporting his research, and had his study been left to circulate in the media unchallenged, we might not have seen the wane in public and political support for capital punishment that we do today.[66]

Data, just like any other valuable resource, can and often does fall into the control of people or organizations that are politically entrenched.[67] Because the legitimacy of discretionary access decisions is not independently scrutinized, restricted access policies allow data producers to withhold information for politically or financially moti-

---

59. Furman v. Georgia, 408 U.S. 238, 240 (1972).

60. Isaac Ehrlich, *The Deterrent Effect of Capital Punishment: A Question of Life and Death*, 65 AM. ECON. REV. 397, 398 (1975).

61. 428 U.S. 153 (1976).

62. *Id.* at 233–34.

63. *See* John J. Donohue & Justin Wolfers, *Uses and Abuses of Empirical Evidence in the Death Penalty Debate*, 58 STAN. L. REV. 791, 793 (2005) (noting that Lawrence Katz, Steven Levitt, Ellen Shustorovich, Hashem Dezhbakhsh, Paul H. Rubin, Joanna M. Shepherd, H. Naci Mocan, R. Kaj Gittings, and Paul R. Zimmerman have written on the issue).

64. *Id.* at 794. Moreover, with so few capital sentences per year the deterrence effects of each capital sentence cannot be disentangled from the year and state controls. *Id.*

65. The Donohue and Wolfers study has been praised by independent reviewers for its use of sensitivity analysis, and for testing findings against alternative specifications and controls. Joshua D. Angrist & Jörn-Steffen Pischke, *The Credibility Revolution in Empirical Economics: How Better Research Design is Taking the Con out of Econometrics* 15 (Nat'l Bureau of Econ. Research, Working Paper No. 15794, 2010), *available at* http://ssrn.com/abstract=1565896.

66. Steve Chapman, *The Decline of the Death Penalty*, CHI. TRIB., Dec. 26, 2010, at C29; Andrew Kohut, *The Declining Support for Executions*, N.Y. TIMES, May 10, 2001, at A33. The empirical research community has seen a similar debate play out in the context of the gun control debate. *See* Ian Ayres & John J. Donohue III, *Shooting Down the "More Guns, Less Crime" Hypothesis*, 55 STAN. L. REV. 1193, 1202 (2003).

67. This phenomenon is, in fact, what motivates George T. Duncan's concept of "information injustice." Duncan, *supra* note 37, at 71, 82.

vated reasons.[68] A thriving public data commons serves the primary purpose of facilitating research, but it also serves a secondary purpose of setting a data-sharing norm so that politically motivated access restrictions will stick out and appear suspect. Thus, if an entity shared data with researchers under a restricted license to support a study that yielded results that happened to harmonize with the entity's self-interest (as was the case when a pharmaceutical company withheld the raw data from its clinical trials even though the results were used to support an application for FDA approval[69]), the lack of transparency would be a signal that the research may have been tainted by significant pressure to come out a particular way.

Today we get the worst of both worlds. Data can be shared through licensing agreements to whomever the data producer chooses, and privacy provides the agency with an excuse beyond reproach when the data producer prefers secrecy to transparency. This is precisely what happened in *Fish v. Dallas Independent School District*.[70] The Dallas School District denied a request from the Dallas chapter of the NAACP for longitudinal data on Iowa Test scores that would have tracked Dallas schoolchildren over an eleven-year period.[71] Based on expert testimony that a malfeasor could "trace a student's identification with the information requested by [the NAACP] using a school directory," the requested data was found to violate FERPA.[72]

The *Fish* opinion interprets and enforces the FERPA regulations properly.[73] The outcome is consistent with FERPA's statutory goals.

---

68. *See* Lawrence O. Gostin, *Health Services Research: Public Benefits, Personal Privacy, and Proprietary Interests*, 129 ANNALS OF INTERNAL MED. 833 (1998).

69. Pub. Citizen Health Research Grp. v. FDA, No. Civ.A. 99-0177(JR), 2000 WL 34262802, at *1 (D.D.C. Jan. 19, 2000) (G.D. Searle & Co. intervened to support the government's decision to withhold clinical trial data based on the privacy exemption in the FOIA statute).

70. 170 S.W.3d 226 (Tex. App. 2005).

71. *Id.* at 227.

72. *Id.* at 230.

73. The requested dataset would have included the sex, age, ethnicity, random teacher code, random school code, test scores, and a few other variables for each student. The request would have revealed PII because the random school and teacher codes, though they sound like *non-identifiers*, are actually *indirect identifiers*. First, the school codes in the Dallas dataset could be cracked using publicly available school enrollment statistics. For example, if Preston Hollow Elementary School was the only school that enrolled 750 students in the year 1995, then its school code could easily be identified by finding the school in the dataset with 750 subjects for the year 1995. Even if two schools happened to have identical enrollment figures for one particular year, the enrollment patterns over time were unique for every school. (The plaintiffs asked for several consecutive years of test scores.) Once the school codes were reverse-engineered, most of the teacher codes could be re-identified using the same methods. Once the school and teacher codes were cracked, Dallas schoolchildren could be organized into small class clusters. A class of thirty schoolchildren cannot be diced into racial groups and gender categories without dissolving into unique cases. *Cf. infra* Part III. This protocol, checking to see whether subgroups of individuals in a dataset could be re-identified using combinations of publicly documented characteristics, is consistent with the directives promulgated by the Family Policy Compliance Office ("FPCO"), the federal agency charged with enforcing FERPA. In providing guidance on the

However, it also exposes the troubling, draconian results of modern data privacy policy. The data requested by the NAACP might have exposed evidence of discrimination or disparate resource allocation. The school district had the option to cooperate with the NAACP's request by using FERPA's research exemption and providing the data under a restrictive license.[74] Alternatively, the district could have provided a randomized sample of the data so that class sizes could not be used to trace identities. But they had little incentive to do either, and perhaps even an incentive *not* to do so. Privacy law provided the school district with a shield from public scrutiny, and allowed the school district to flout the objectives of public records laws.

We will never know what the *Fish* data might have revealed. Perhaps theories of disparate treatment across class or race lines would have been borne out. Perhaps the research would have facilitated some other, unanticipated finding. Even the confirmation of a null hypothesis can have significant implications, particularly where a portion of the population suspects it may be receiving inequitable treatment. Since privacy law allowed the data producer to avoid disclosure, the value of the withheld data will be forever obscured, and any systemic patterns will be known only to the Dallas school district — if they are known at all. The *Fish* case nicely illustrates the dangers of assigning too little value to research data in the abstract.

E. Freedom of Information Act Requests: Privacy as an Evasion Technique

We would expect public agencies, which are subject to strong public access obligations from FOIA and state public records statutes,[75] to have fewer opportunities to make improperly motivated access decisions. After all, one of the primary goals of public access statutes is to take decisions about who does and does not get to access information out of the hands of the agency.[76] But increased anxieties over the theoretical risk of re-identification arm government agencies with a pretext for denying records requests. As Douglas Sylvester and

---

scope of "personally identifiable information," the FPCO opined that under certain circumstances "the aggregation of anonymous or de-identified data into various categories could render personal identity 'easily traceable.' In those cases, FERPA prohibits disclosure of the information without consent." *See* Letter from LeRoy S. Rooker, Director, Family Policy Compliance Office, to Corlis P. Cummings, Senior Vice Chancellor for Support Services, Bd. of Regents of the Univ. Sys. of Ga. (Sept. 25, 2003), *available at* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/georgialtr.html.

74. 20 U.S.C. § 1232g(b)(1)(F) (2006).

75. *See, e.g.*, Freedom of Information Act, 5 U.S.C. § 552 (2006); California Public Records Act, CAL. GOV'T CODE §§ 6250 et seq. (West 2008); Freedom of Information Law, N.Y. PUB. OFFICERS LAW §§ 84 et seq. (Consol. 2011).

76. *See, e.g.*, CAL. GOV'T CODE § 6250 (West 2011) ("[A]ccess to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state.").

Sharon Lohr have noted, "the strengthening of individual rights-based privacy has allowed some agencies to use privacy as a 'shield' to prevent otherwise appropriate disclosures."[77] The moral hazard reached its apex under the Bush Administration, which shielded the records of current and past presidents from FOIA requests through executive order.[78] The exemption was voluntarily repealed in 2009.[79]

This is not to say that every denial of a public records request is made in bad faith. A number of structural problems plague the process and encumber disclosure. First, the lack of comprehensible standards for privacy protocols (discussed at length in Part V) will tend to drive state agencies to withhold data from researchers if disclosure exposes the agency to liability or sanction. Moreover, the penalties and public criticism for releasing ineffectively anonymized information are much harsher than the consequences of improperly denying a public records request.[80] The imbalanced structural incentives obscure and exacerbate the potential for self-serving behavior. Freedom of information advocates and professional journalism associations allege that privacy exemptions, like national security exemptions, are abused when the requested information is embarrassing for the agency.[81] Thus, as the Society of Professional Journalists puts it, rich data is disclosed about tomato farming and transportation, while data that could be used to vet a government program or expose agency wrongdoing is redacted into oblivion — if it is released at all.[82]

Numerous examples from the FOIA case law support these observations. The Department of Agriculture used the privacy exemption of FOIA to deny a request for the identity of a corporation that compensated or bribed a member of the Dietary Guidelines Advisory Committee.[83] The State Department refused to release documents about forcibly repatriated Haitian refugees to human rights groups — purportedly to protect their privacy.[84] Privacy was "feebly" held up as a justification for declining to collect information about the religious exercise of Navy personnel, in an attempt to rebut a group of Navy chaplains' allegations that nonliturgical Christians were disfavored and underrepresented in the Navy's decisions about hiring, promotion,

77. Sylvester & Lohr, *supra* note 12, at 190; *see also* Cate, *supra* note 9, at 13–15.

78. Further Implementation of the Presidential Records Act, Exec. Order No. 13233, 66 Fed. Reg. 56,025 (Nov. 5, 2001).

79. Presidential Records, Exec. Order No. 13489, 74 Fed. Reg. 4669 (Jan. 21, 2009).

80. For example, in Arizona, improper disclosure of private facts is a felony, while improper denial of a legitimate public records request is a misdemeanor. *See Air Talk: The "Open Government Plan"* (Southern California Public Radio broadcast Dec. 14, 2009), *available at* http://www.scpr.org/programs/airtalk/2009/12/14/the-open-government-plan.

81. *Id.*

82. *Id.*

83. Physicians Comm. for Responsible Med. v. Glickman, 117 F. Supp. 2d 1, 5–6 (D.D.C. 2000).

84. U.S. Dep't of State v. Ray, 502 U.S. 164, 166 (1991).

and retention.[85] In each of these examples, the government's privacy argument eventually failed. But sometimes this argument prevails.[86] And a great majority of denials of public records requests are not litigated at all.[87]

In 2008, UCLA denied a public records request that a faculty member on the undergraduate admissions committee submitted for the University's admissions data.[88] UCLA concluded that the request posed "serious privacy concerns" and could not be fulfilled without violating FERPA.[89] Astonishingly, the same rationale did not impede UCLA from sharing similar admissions data under a restricted license agreement to a different UCLA professor.[90] The only appreciable difference between the two requests was the divergent attitudes each professor maintained toward UCLA's admissions process. The denied requester openly questioned whether the school was using applicant race information in an impermissible way.[91]

The University of Arkansas Little Rock ("UALR") School of Law denied a similar request for admissions data from a faculty member on its admissions committee. The professor regularly reviewed the original, raw admissions files, but the school denied his request for data, claiming that FERPA prohibited the release of even de-identified statistical data.[92] When a UALR Law School alumna requested access to similar application data in an independent request, the University (perhaps inadvertently) disclosed a memorandum of notes documenting advice from their legal counsel: "We say FERPA, they can challenge if they want."[93] A cogent interpretation is that the federal privacy law is being used as a tactical device to greatly increase the transaction costs for public records requests. Since requests for anonymized university and law school admissions data have already passed judicial scrutiny assessing FERPA compliance,[94] the general

85. Adair v. England, 183 F. Supp. 2d 31, 56 (D.D.C. 2002).

86. *See* Fish v. Dallas Indep. Sch. Dist., 170 S.W.3d 226 (Tex. App. 2005).

87. COALITION OF JOURNALISTS FOR OPEN GOV'T, FOIA LITIGATION DECISIONS, 1999–2004 1 (2004), *available at* http://www.cjog.net/documents/Litigation_Report_9904.pdf.

88. TIMOTHY GROSECLOSE, CUARS RESIGNATION REPORT (2008), *available at* http://images.ocregister.com/newsimages/news/2008/08/CUARSGroseceloseResignationReport.pdf; *see also* Seema Mehta, *UCLA Accused of Illegal Admitting Practices*, L.A. TIMES, Aug. 30, 2008, at B1.

89. *See* GROSECLOSE, *supra* note 88.

90. *Id.*

91. *Id.*

92. Robert Steinbuch, What They Don't Want Me (and You) to Know About Non-Merit Preferences in Law School Admissions: An Analysis of Failing Students, Affirmative Action, and Legitimate Educational Interests 3 (unpublished manuscript) (on file with author).

93. Richard J. Peltz, *From the Ivory Tower to the Glass House: Access to "De-Identified" Public University Admission Records to Study Affirmative Action*, 25 HARV. J. ON RACIAL & ETHNIC JUSTICE 181, 185–87 (2009).

94. *See, e.g.*, Osborn v. Bd. of Regents of Univ. of Wis., 647 N.W.2d 158, 171 (Wis. 2002) ("[B]y redacting or deleting the name of the high school or undergraduate institution, the University no longer faces a situation where only one minority student from a named

counsel's offices at UCLA and UALR ought to have known that, with minimal effort, a sufficiently safe admissions dataset could be produced.

The distribution of access to data is a problem worthy of national attention and concerted effort. The data commons is a powerful, natural antidote to information abuses. It is critical for information justice, since our pooled data can reveal the patterns of human experience that no single anecdote can. Since the value of a dataset cannot be determined ex ante, any rule that significantly impedes the release of research data imposes a social cost of uncertain magnitude.

III. DOOMSDAY DETECTION: THE COMPUTER SCIENCE APPROACH

A large body of computer science literature explores the theoretical risk that a subject in an anonymized dataset can be re-identified. De-anonymization scientists study privacy from an orientation that emphasizes any harm that is theoretically possible. They are in the habit of looking for worst-case scenario risks.[95] This orientation grows out of a natural inclination to believe that, if there is value to abusing anonymized data, and if re-identification is not too difficult, then such re-identification will happen. In other words, where there is motive and opportunity, a de-anonymization attack is a foregone conclusion. The de-anonymization scientists' perspective has some intuitive appeal, and the legal literature has embraced the findings and predictions of the computer science literature without much skepticism.[96] The de-anonymization literature taps into privacy advocates' natural unease any time information is distributed without the consent of the data subjects.

In this Part, I briefly explain how de-anonymization attacks work.[97] Next, I explore the lessons growing out of the computer science literature and find that they greatly exaggerate the opportunities and motivations of the hypothetical adversary. The computer science

high school applies to one of the University's campuses and therefore, even though the student's name is not disclosed, the data could be personally identifiable.").

95. Mark Elliot, *DIS: A New Approach to the Measurement of Statistical Disclosure Risk*, 2 RISK MGMT. 39 (2000) (putting forward a new method of measuring the "worst-case risk"); Jordi Nin et al., *Rethinking Rank Swapping to Decrease Disclosure Risk*, 64 DATA & KNOWLEDGE ENGINEERING 346 (2008). But note that many computer scientists also incorporate assessments of data utility and information loss into their work. *See, e.g.*, DUNCAN, *supra* note 11; Josep Domingo-Ferrer et al., *Comparing SDC Methods for Microdata on the Basis of Information Loss and Disclosure Risk*, EUROPEAN COMMISSION (2001), http://epp.eurostat.ec.europa.eu/portal/page/portal/research_methodology/documents/81.pdf.

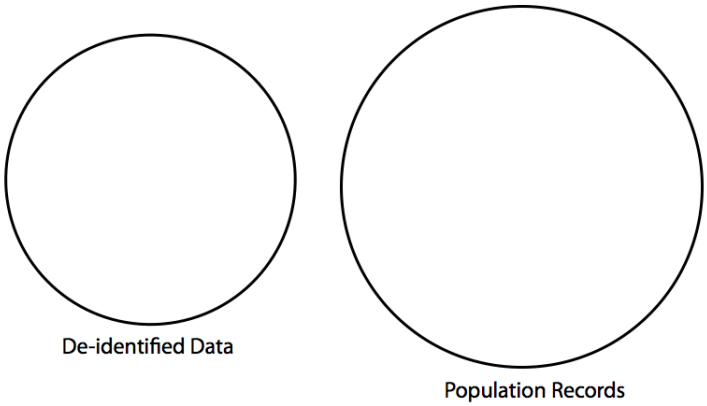
96. *See infra* notes 117–119, 135 and accompanying text.

97. For a concise overview on how de-anonymization attacks work, see JANE YAKOWITZ & DANIEL BARTH-JONES, TECH. POLICY INST., THE ILLUSORY PRIVACY PROBLEM IN *SORRELL V. IMS HEALTH* 1–5 (2011), http://www.techpolicyinstitute.org/files/the%20illusory%20privacy%20problem%20in%20sorrell1.pdf.

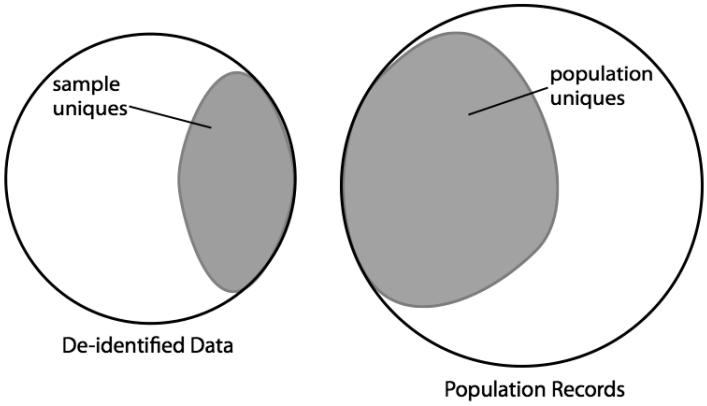
literature (and the policymakers who borrow from it) makes five inaccurate assertions: (1) every variable in a dataset is an indirect identifier; (2) data supporting inferences about a population of data subjects violates privacy; (3) useful data is necessarily privacy-violating; (4) re-identification techniques are easy; and (5) public datasets have value to an adversary over and above the information he already has. I will address each of these in turn.

A. How Attack Algorithms Work

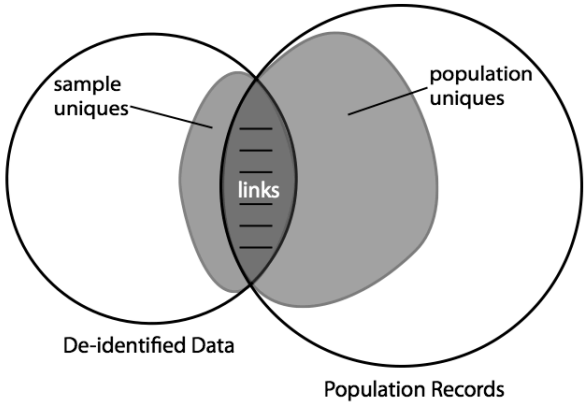
All de-anonymization attack algorithms are variants of one basic model. An adversary attempts to link subjects in a de-identified database to identifiable data on the entire relevant population ("population records"). The adversary links the two databases using indirect identifier variables that the two datasets have in common. To visualize the attack, suppose the two circles in this diagram represent the indirect identifiers in the de-identified database and the population records, respectively. Initially, these databases have no linkages:



The adversary identifies subjects in the de-identified data that have a unique combination of values among the indirect identifiers. He does the same to the population records:



Finally, the adversary links all the sample uniques he can to the population uniques:



Only a subset of the sample uniques and population uniques will be linkable because some of the sample uniques might not actually be unique in the population, and some of the population uniques might not be present in the sample of the de-identified data.[98]

98. More sophisticated techniques will make matches not based on strong exact linkages but on the similarity of the matching variables and the greater deviation between the best match and the second-best match. This allows an attack algorithm to make matches under more realistic conditions in which databases contain measurement error, but it nevertheless requires that the adversary have access to more-or-less complete information on the general

Latanya Sweeney provided the classic example of a successful matching attack when she combined de-identified Massachusetts hospital data with identifiable voter registration records in order to re-identify Governor William Weld's medical records.[99] Because the hospital data at that time — before the passage of HIPAA — included granular detail on the patients (5-digit ZIP code, full birth date, and gender), many patients were unique in the hospital data and the voter records.

Today, there is little disagreement that this sort of "trivial de-identification" of records — the removal of only direct identifiers like names, social security numbers, and addresses — is insufficient on its own. Subjects can too easily be identified through a combination of indirect identifiers. Thus, like other federal privacy statutes, HIPAA requires data producers to remove not only the obvious direct identifiers, but also *any* information known by the disclosing agency that can be used alone or in combination with other information to identify an individual subject.[100]

While there is broad agreement on the rejection of trivial de-identification, privacy experts disagree on the efficacy of current best practices. Legal scholars and advocacy groups limit their focus to the computer science studies falling on one side of the debate — those making the common erroneous assertions explored below — while ignoring the disclosure-risk research coming out of the statistical and public health disciplines. This has had the unfortunate consequence of leading the legal and policy discourse astray.

B. Erroneous Assertions

The mounting literature on privacy risks associated with anonymized research data propagates five myths about re-identification risk. In combination, these inaccurate assertions lead lay audiences to believe that anonymized data cannot be safe.

1. Not Every Piece of Information Can Be an Indirect Identifier

Disclosure risk analysis has traditionally looked for categories of information previously disclosed to the public in order to distinguish "indirect identifiers" from "non-identifiers." For example, data subjects' names and addresses are available in voter registration rosters

---

population from which the de-identified data was sampled. These methods are described more thoroughly by Josep Domingo-Ferrer et al., *supra* note 95, at 813–14.

99. *See* Sweeney, *supra* note 11, at 52.

100. HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.514(b)(2)(ii) (2010). Alternatively, the disclosing entity must use "generally accepted statistical and scientific principles and methods" to ensure that the risks of re-identification are "very small." § 164.514(b)(1).

(which are public records); therefore ZIP codes and other geographic codes must be classified as indirect identifiers.[101] On the other hand, food preferences are not systematically collected and re-released publicly, so a variable describing the subject's favorite food would traditionally be considered a non-identifier.

De-anonymization scientists do not limit the theoretical adversary to public sources of information. The most influential de-anonymization study, by Arvind Narayanan and Vitaly Shmatikov, describes the re-identification of subjects in the Netflix Prize Dataset.[102] In 2006, Netflix released an anonymized dataset to the public consisting of movie reviews of 500,000 of its members.[103] Narayanan and Shmatikov used information from user ratings on the Internet Movie Database (IMDb) to re-identify subjects in the Netflix Prize dataset.[104] This study is regarded as proof that publicly accessible datasets can be reverse-engineered to expose personal information even when state-of-the-art anonymization techniques are used.[105] The study energized the press because the auxiliary information Narayanan and Shmatikov used was collected from the Internet. But before diving into how the algorithm works, it is helpful to note a chasm between Narayanan and Shmatikov's conception of privacy risk and that enshrined in U.S. privacy statutes.

Narayanan and Shmatikov examine how auxiliary information learned through any means at all, even at the water cooler, could be used to identify a target.[106] They ask, "if the adversary knows a few of the [target] individual's purchases, can he learn *all* of her purchases?" and "if the adversary knows a few movies that the individual watched, can he learn *all* movies she watched?"[107] The implicit directive from these questions is that public datasets must be immune from targeted attacks using special information. The belief that privacy policy is expected to protect data even from snooping friends and coworkers is

---

101. *What is a Quasi-identifier?*, ELECTRONIC HEALTH INFO. LABORATORY (Oct. 18, 2009), http://www.ehealthinformation.ca/knowledgebase/article/AA-00120. Note that indirect identifiers are also known as "quasi-identifiers."

102. Narayanan & Shmatikov, *supra* note 11.

103. *Id.*

104. *Id.* at 122–23. The authors first mapped the five-point scale from Netflix movie ratings onto the ten-point scale used by IMDb, and then attempted to identify matches based on strings of movies that were reviewed similarly on both websites. *Id.*

105. Brief of *Amicus Curiae* Electronic Frontier Foundation in Support of Petitioners at 9–10, Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (2011) (No. 10-779), 2011 WL 757416, at *9–10; *see also supra* note 5 (discussing various privacy lawsuits). Netflix had added random noise to the dataset. Narayanan & Shmatikov, *supra* note 11, at 119.

106. *See* Narayanan & Shmatikov, *supra* note 11, at 122 ("A water-cooler conversation with an office colleague about her cinematographic likes and dislikes may yield enough information [to de-anonymize her subscriber record] . . . .").

107. *Id.* at 112; *see also* Cynthia Dwork, *Differential Privacy*, 2006 PROC. 33RD INT'L COLLOQUIUM ON AUTOMATA, LANGUAGES & PROGRAMMING, *available at* http://research.microsoft.com/pubs/64346/dwork.pdf.

adopted reflexively by Paul Ohm without acknowledging that it introduces a significant departure from the design of current law: "To summarize, the next time your dinner party host asks you to list your six favorite obscure movies, unless you want everybody at the table to know every movie you have ever rated on Netflix, say nothing at all."[108] If public policy had embraced this expansive definition of privacy — that privacy is breached if somebody in the database could be re-identified by anybody else using special non-public information — dissemination of data would never have been possible. Instead, U.S. privacy law in its various forms requires data producers to beware of indirect identifiers that are, or foreseeably could be, in the public domain.[109]

However, Narayanan and Shmatikov's study has sway because the Internet gives a malfeasor access to more information than he ever had before. Narayanan and Shmatikov were able to use the IMDb movie reviews of two strangers to re-identify them in the Netflix data.[110] Their study illustrates how the Internet is a (relatively) new public information resource that blurs the distinction between non-identifiers and indirect identifiers.[111] The Internet affects data anonymization by archiving and aggregating large quantities of information and by making information gathering practically costless.[112] It also provides a platform for self-revelation and self-publication, making the available range of information about any one person unpredictable and practically limitless.

Current privacy policy does not anticipate how we should deal with this shift. On one hand, if anybody can access information on the Internet, it seems unquestionable that the information is "public." Thus, this information might best be described as an indirect identifi-

---

108. Ohm, *supra* note 4, at 1721.

109. For example, regulations issued under FERPA define PII to include "information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, *who does not have personal knowledge of the relevant circumstances*, to identify the student with reasonable certainty." 34 C.F.R. § 99.3 (2011) (emphasis added). Likewise, "[a]t a minimum, each statistical agency must assure that the risk of disclosure from the released data when combined with other relevant *publicly available* data is very low." *Report on Statistical Disclosure Limitation Methodology* 3 (Fed. Comm. on Statistical Methodology, Statistical Working Paper No. 22, 2d version, 2005) [hereinafter Working Paper No. 22] (emphasis added), *available at* http://www.fcsm.gov/working-papers/SPWP22_rev.pdf.

110. Narayanan & Shmatikov, *supra* note 11, at 123.

111. *See generally id.* Narayanan and Shmatikov make similar breakthroughs using graphs of network connections of anonymized Twitter accounts by matching them to sufficiently unique networked accounts on Flickr. Arvind Narayanan & Vitaly Shmatikov, *Deanonymizing Social Networks*, 2009 PROC. 30TH IEEE SYMP. ON SECURITY & PRIVACY 173.

112. Schwartz, *supra* note 6; Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1185 (2002) ("The aggregation problem arises from the fact that the digital revolution has enabled information to be easily amassed and combined.").

er. On the other hand, data sharing will be severely constrained if the status of a category of information is shifted from non-identifier to indirect identifier simply because members of a small minority of data subjects choose to reveal information about themselves. If I blog about a hospital visit, should my action render an entire public hospital admissions database (relied on by epidemiologists and health policy advocates) in violation of privacy law? Are the bounds of information flow really to be determined by the behavior of the most extroverted among us?[113] This looks like a quagmire from which no reasonable normative position can emerge.[114] The approach that I endorse in Part V sidesteps this question because the issue does not become relevant until we reach the apocalyptic scenario in which reidentification is a plausible risk, and adversaries painstakingly troll through our blogs to put together complete dossiers. For reasons that will soon become evident, such adversaries are unlikely to materialize.

The Netflix study makes an excellent contribution to our knowledge base, but it is a theoretical contribution. The Narayanan-Shmatikov de-anonymization algorithm is limited to a set of anonymized datasets with particular characteristics. For the algorithm to work, the dataset must be large (in the sense of having a large number of variables or attributes), and it must be sparse (which is a technical term roughly meaning that most of the dataset is empty, and that the data subjects are readily distinguishable from each other).[115] Moreover, because the attack algorithm infers population uniqueness from sample uniqueness, the research dataset must have accurate and complete information about the data subjects in the sample in order to avoid false positives and negatives[116] — a condition that does not

113. As Andrew Serwin puts it, "[i]ndeed, in today's Web 2.0 world, where many people instantly share very private aspects of their lives, one can hardly imagine a privacy concept more foreign than the right to be let alone." Andrew Serwin, *Privacy 3.0 — The Principle of Proportionality*, 42 U. MICH. J. L. REFORM 869, 872 (2009).

114. Indeed, "lifelogging" on the Internet presents a number of challenges for privacy scholars even on their own. Anita Allen has written about the problems of the Internet's "pernicious memory" recalling information that puts the lifelogger in the worst light. Anita L. Allen, *Dredging Up the Past: Lifelogging, Memory, and Surveillance*, 75 U. CHI. L. REV. 47, 56–63 (2008).

115. *See* Narayanan & Shmatikov, *supra* note 11, at 111.

116. The Narayanan-Shmatikov algorithm utilizes the dataset's sparseness to test for false positive matches. If a set of movies leads to a unique match in the Netflix data, and if the movies don't share a common fan base, then the algorithm will be confident that the match is accurate. *Id.* at 112. But the Netflix Data is missing a lot of information about the movie-viewing of its own data subjects. The algorithm is susceptible to false positives and false negatives when it attempts to match against auxiliary information. Take this simplified but illustrative hypothetical: Albert, Bart, and Carl have all seen *Doctor Zhivago*, *Evil Dead II*, and *Dude, Where's My Car?*. Albert and Bart are in the Netflix database, Carl is not. Albert rates all three movies, but Bart rates only *Doctor Zhivago*, and, thus, Netflix has no record of his having seen *Evil Dead II* and *Dude, Where's My Car?*. Because Albert is the only person in the Netflix dataset who rated all three movies, he looks highly unique among

even hold for the Netflix data and is certainly not characteristic of most large commercial datasets, such as consumer data from Amazon. And, importantly, the adversary must understand entropic de-anonymization in order to test the confidence level of his algorithm's match.

These limitations are sizeable, yet they are entirely ignored by the legal scholars, privacy advocates, civil litigants, and now, the FTC, relying on the study to conclude that anonymization is dead.[117] The Narayanan-Shmatikov study has provided the first ping in an echo chamber that has distorted the conversation about public research data. Consider, for example, this report prepared by the preeminent privacy scholar Paul Schwartz:

> Regarding the question of PII versus non-PII, recent work in computer science has shown how easy it can be to trace non-PII to identifiable individuals . . . . [A] study involving Netflix movie rentals was able to identify *eighty percent* of people in a supposedly anonymous database of 500,000 Netflix users; the identification was triggered by their ratings in the Netflix database of at least three films.[118]

The Electronic Privacy Information Center ("EPIC") has gone further, claiming that the study authors re-identified 99 percent of the Netflix users.[119] These statements bear scant relation to reality. In fact, Narayanan and Shmatikov performed a proof of concept study on a small sample of IMDb users. They successfully re-identified two of the IMDb users in the Netflix database.[120] There is a real risk that the

---

the Netflix data subjects, even though we know, in fact, that these three movies are not unique to him even within the Netflix sample. Carl comments on all three movies on IMDb. The attack algorithm matches Carl's IMDb profile to Albert's Netflix data and reports back with a high degree of statistical confidence that the match is not a false positive.

117. In January 2010, a panel of privacy law experts and computer scientists advised the FTC that, in promulgating new regulations, it should abandon faith in anonymization and clamp down on broad data sharing to the extent possible. The Narayanan-Shmatikov study was held up as evidence that anonymization protocols offer no security against re-identification. Remarks at the FTC Second Roundtable on Exploring Privacy 15, 56 (Jan. 28, 2010) (transcript available at http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.pdf). Narayanan, however, cognizant of the importance of research data, has worked with entities to anonymize public release datasets sufficiently to reduce risks. *See* Steve Lohr, *The Privacy Challenge in Online Prize Contests*, N.Y. TIMES BITS (May 21, 2011, 5:25 PM), http://bits.blogs.nytimes.com/2011/05/21/the-privacy-challenge-in-online-prize-contests.

118. SCHWARTZ, *supra* note 12, at 7 (emphasis added).

119. Brief of Amici Curiae Electronic Privacy Information Center (EPIC) et al. in Support of the Petitioners at 33, Sorrell v. IMS Health, Inc., 131 S. Ct. 2653 (2011) (No. 10-779), *available at* http://www.scotusblog.com/case-files/cases/sorrell-v-ims-health-inc.

120. Narayanan & Shmatikov, *supra* note 11, at 122–23.

echo chamber will continue to distort the reasoned judgment of lawmakers and regulators if such misconceptions are not corrected now.

Of the studies conducted in the last decade, only one was conducted under the conditions that replicate what a real adversary would face while also verifying the re-identifications. The Federal Department of Health and Human Services Office of the National Coordinator for Health Information Technology ("ONC") put together a team of statistical experts to assess whether data properly de-identified under HIPAA can be combined with readily available outside data to re-identify patients.[121] The team began with a set of approximately 15,000 patient records that had been de-identified in accordance with HIPAA.[122] Next, they sought to match the de-identified records with identifiable records in a commercially available data repository and conducted manual searches through external sources (e.g., InfoUSA) to determine whether any of the records in the identified commercial data would align with anyone in the de-identified dataset.[123] The team determined that it was able to accurately re-identify two of the 15,000 individuals, for a match rate of 0.013%.[124] In other words, the risk — even after significant effort — was very small.[125]

Other, less attention-grabbing studies from the field of statistical disclosure risk have similarly differed from the conclusions drawn by the Narayanan-Shmatikov study: in realistic settings, datasets can rarely be matched to one another because both sets of data usually contain substantial amounts of measurement error that decimate the opportunity to link with confidence.[126] This is not the sort of difficulty that can be overcome with technology or shrewd new attack techniques; rather, it is a natural protection afforded by the inherently messy nature of data and of people.[127]

2. Group-Based Inferences Are Not Disclosures

Computer scientists have an expansive definition of privacy. They count as privacy breaches even mere inferences that might be applied to an individual based on subgroup statistics. Justin Brickell and

121. Deborah Lafky, Dep't of Health and Human Servs. Office of the Nat'l Coordinator for Health Info. Tech., The Safe Harbor Method of De-Identification: An Empirical Test 15–19 (2009), http://www.ehcca.com/presentations/HIPAAWest4/lafky_2.pdf.

122. *Id.* at 16.

123. *Id.* at 17–18.

124. *Id.* at 19.

125. These findings are consistent with an earlier study that examined re-identification attacks under realistic conditions. *See* U. Blien et al., *Disclosure Risk for Microdata Stemming from Official Statistics*, 46 STATISTICA NEERLANDICA 69 (1992).

126. *See id.* at 80–81.

127. Even under conditions that are considered risky, re-identification of anonymized datasets is difficult to pull off due to the "natural unreliability of measurement," which serves as a natural barrier. Walter Müller, et al., *Identification Risks of Microdata*, 24 SOC. METHODS & RES. 131, 151 (1995).

Vitaly Shmatikov, computer scientists at the University of Texas whose work has greatly influenced Paul Ohm's scholarship, define privacy breach to include the release of any information where the distribution of a sensitive variable for a subgroup of data subjects differs from that variable's distribution over the entire sample.[128] Similarly, Cynthia Dwork has crafted her definition of "differential privacy" to cover group privacy.[129]

This conception of a privacy right — one that protects against the disclosure of any sensitive information that differs by demographic subgroup — avoids two potential harms that can result from group inference disclosure. First, facts about a group can be used to make a determination about an individual. For example, a health care provider might deny coverage to a member of a particular subgroup based on the health profiles of the entire subgroup. Second, group differences in a sensitive characteristic can lead the public to adopt inappropriate stereotypes that mischaracterize individuals and lead to prejudices. James Nehf describes the problem as so: "Since the information used to form [a] judgment is not the complete set of relevant facts about us, we can be harmed (or helped) by the stereotyping or mischaracterization."[130]

These criticisms are shortsighted. They are, in fact, attacks on the very nature of statistical research. Federal statistical agencies have responded to concerns about subgroup inference disclosure with two persuasive retorts. "First[,] a major purpose of statistical data is to enable users to infer and understand relationships between variables. If statistical agencies equated disclosure with inference, very little data would be released."[131] Indeed, the definition of privacy breach used by Brickell and Shmatikov is a measure of the data's utility; if there are group differences between the values of the sensitive variables, such as a heightened risk of cancer for a discernable demographic or geographic group, then the data is likely to be useful for exploring and understanding the causes of those differences.[132]

---

128. Justin Brickell & Vitaly Shmatikov, *The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing*, 2008 PROC. 14TH ACM SIGKDD INT'L CONF. ON KNOWLEDGE DISCOVERY & DATA MINING (KDD) 70, 72; *see also* Narayanan & Shmatikov, *supra* note 11, at 114.

129. Dwork, *supra* note 107, at 9.

130. James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 24 (2003). Similar arguments have arisen in response to the disclosure of information about Tay-Sachs disease in the Jewish community and sickle-cell anemia in the African-American population. Lawrence O. Gostin & Jack Hadley, *Health Services Research: Public Benefits, Personal Privacy, and Proprietary Interests*, 129 ANNALS OF INTERNAL MED. 833, 834 (1998).

131. Working Paper No. 22, *supra* note 109, at 11.

132. I discuss in Part IV how the Brickell and Shmatikov definition of privacy has misled legal scholars to believe that there is a forced choice between privacy and data utility.

"Second, inferences are designed to predict aggregate behavior, not individual attributes, and thus are often poor predictors of individual data values."[133] That is to say, the use of aggregate statistics to judge or make a determination on an individual is often inappropriate. Though stereotyping might happen anyway, it has never been a goal of privacy law to prevent all forms of ignorant speculation. Stereotyping will not go away by suppressing data. To the contrary, data can be very useful in debunking stereotypes.[134]

3. A Data Release Can Be Useful and Safe at the Same Time

Paul Ohm argues that if data is useful to researchers, it must create a serious risk of re-identification.[135] This claim has been repeated in the national media.[136] But the assertion is erroneous. A database with just one indirect-identifying variable (such as gender) tied to non-public information (such as pharmaceutical purchases) can be tremendously valuable for a *specific* research question — such as: "Do women purchase drugs in proportion to the national rates of diagnosis?" — without any risk of re-identification. Ohm and the media outlets were thrown off because the technical studies they cite use a definition of data-mining utility that encompasses *all possible* research questions that could be probed by the original database.[137] So, for example, if race and geographic indicators are removed from the database, the utility of that database for all possible research questions plummets, even though the utility of that database for this specific research question stays intact. For specific research questions, utility and anonymity can and often do coexist.

133. Working Paper No. 22, *supra* note 109, at 11.

134. To the very limited extent group inference privacy has been tested in the courts, judges have been unwilling to recognize an implied contract or privacy challenge to releases of de-identified data, even when the de-identified data could be used to make group inferences for marketing purposes. *See* London v. New Albertson's, Inc., No. 08-CV-1173 H(CAB), 2008 WL 4492642, at *5–6 (S.D. Cal. Sept. 30, 2008) (holding that the disclosure of anonymous individual-level pharmacy patient data to a marketing firm did not contravene assurances from a pharmacy that it "collects your personal information and prescription information only for the fulfillment of your prescription order and to enable you to receive individualized customer service beyond what we can provide to anonymous users").

135. Ohm, *supra* note 4, at 1755.

136. Singel, *supra* note 5.

137. *See* Brickell & Shmatikov, *supra* note 128, at 74. The study does helpfully prove that small increases in privacy protection cause disproportionately large destruction of overall utility. *Id.* at 78. But if privacy protocols are designed to preserve the utility of a dataset for a *particular* research question, nothing in the study suggests that this would not be possible.

4. Re-Identifying Subjects in Anonymized Data Is Not Easy

Computer scientists concerned about data privacy face the challenge of convincing the public that an adversary of low-to-moderate skill is capable of performing the same sort of attacks that they can. De-anonymization scientists often refer to the fact that their attacks can be performed on home computers using popular programs.[138] Paul Ohm makes the same rhetorical move in order to argue that we are living in the era of "easy reidentification."[139]

> The Netflix study reveals that it is startlingly easy to reidentify people in anonymized data. Although the average computer user cannot perform an inner join, most people who have taken a course in database management or worked in IT can probably replicate this research using a fast computer and widely available software like Microsoft Excel or Access.[140]

While the Netflix attack algorithm could be performed using Excel, an adversary would have to understand the theory behind the algorithm in order to know whether the dataset is a good candidate and whether matches should be rejected as potential false positives.[141] The suggestion that anybody with an IT background and a copy of Excel can do this is implausible.

The myth of easy re-identification was tested and rejected in the case of *Southern Illinoisan v. Illinois Department of Public Health*.[142] In that case, the plaintiff newspaper submitted a public records request to the Illinois Department of Public Health for a table containing the ZIP codes, dates of diagnosis, and types of cancer for hospital patients in the department's database.[143] The plaintiff newspaper's goal was to test whether certain forms of cancer were clustered in distinct geographic areas,[144] which would have suggested that their incidence was created or greatly exacerbated by environmental factors.[145] The government relied on the testimony of Dr. Latanya Sweeney to support its argument that granting the request would violate cancer patient privacy because the data could be de-anonymized.[146]

---

138. *See, e.g.*, S. Illinoisan v. Ill. Dep't of Pub. Health, 844 N.E.2d 1, 7 (Ill. 2006).
139. Ohm, *supra* note 4, at 1716.
140. *Id.* at 1730 (footnote omitted).
141. *See supra* text accompanying notes 115–116.
142. 844 N.E.2d 1.
143. *Id.* at 3.
144. *Id.*
145. *See id.* at 7.
146. *Id.* at 4. The privacy standard for this case was heightened from PII to information that "*tends* to lead to the identity." *Id.* at 18 (emphasis added). Nevertheless the court found that the government failed to demonstrate that the requested data would tend to lead to the

Dr. Sweeney's testimony about the process she used to re-identify subjects is under seal out of a fear that the opinion would create an instruction book for a true malfeasor,[147] but the description in the Illinois Supreme Court's opinion suggests that she did the following[148]: She began by researching the disease of neuroblastoma — the rare form of cancer of interest to the plaintiff newspaper — in order to familiarize herself with the symptoms and treatment.[149] Next, she purchased two thousand dollars' worth of public and "semi-public" datasets, some of which required her to fill out forms and wait for processing.[150] Some of these purchased datasets (probably voter registration data) identified their subjects by name and address.[151] If Dr. Sweeney employed the same processes that she had previously used to re-identify health records, it is very likely that she linked the identifiable data to pre-HIPAA hospital discharge data that had not been anonymized (only the names had been removed) by using granular detail about the hospital patients' dates of birth, sex, and ZIP codes.[152] Since the passage of HIPAA, such information is no longer publicly available.[153] Next, Dr. Sweeney used what she learned about neuroblastoma to identify possible neuroblastoma patients in the combined purchased databases.[154] The purchased data contained some information — secondary diagnoses or prescription drug treatments perhaps — that allowed her to infer which people in the consumer databases suffered from neuroblastoma.[155] Since the purchased public data was linked to identities, she was able to use what she learned from the purchased resources to produce accurate names for most of the entries in the requested cancer registry dataset.[156]

Dr. Sweeney testified that it would be very easy for anyone to identify people in the cancer registry dataset:

> It is very easy in the following sense, all I used was commonly available PC technology . . . [a]nd readily available software . . . and all that was required were the simple programs of using [spreadsheets]. . . . They come almost on every machine now days

identities of the subjects. *Id.* at 21. Before she took the witness stand in this case, Dr. Sweeney had demonstrated that re-identification of allegedly anonymized data was possible by reverse-engineering Massachusetts medical data. *See* Sweeney, *supra* note 11.

147. *S. Illinoisan*, 844 N.E.2d at 7–8.
148. *Id.* at 8.
149. *Id.*
150. *Id.*
151. *Id.* at 4.
152. *See* Sweeney, *supra* note 11.
153. 45 C.F.R. § 164.514(b)(2)(i) (2010).
154. *S. Illinoisan*, 844 N.E.2d at 8.
155. *Id.*
156. *Id.*

> [sic] . . . so they don't require you have [sic] any programming or require you to take a computer class, but they do require you to know the basics of how to use the machine and how to use those simple packages.[157]

The Illinois Supreme Court was not convinced. The court reasoned that it was Dr. Sweeney's "'knowledge, education and experience in this area' that made it possible for her to identify the Registry patients" and not merely her access to Microsoft Excel.[158] Because Dr. Sweeney used her well-honed discretion to make matches between two data sources that did not map easily onto each other, Dr. Sweeney's methods took advantage of her efforts and talents. *Southern Illinoisan* and the Netflix example illustrate that designing an attack algorithm that sufficiently matches multiple indirect identifiers across disparate sources of information, and assesses the chance of a false match, may require a good deal of sophistication.

5. De-Anonymized Public Data Is Not Valuable to Adversaries

The plaintiffs in *Southern Illinoisan* had a second objection to Dr. Sweeney's testimony: Dr. Sweeney identified neuroblastoma patients using the purchased data resources, not the dataset requested by the plaintiffs.[159] She used the requested table "only to verify her work"[160]: she checked to see if the ZIP codes and diagnosis dates of her neuroblastoma candidate guesses matched the anonymous cancer registry.[161]

The requested table undoubtedly provided some value by allowing her to have more confidence in the attack algorithm. However, the added utility to an adversary in this situation, as compared to what the adversary could have done without the requested table, was very small.[162] Whether the anticipated abuse is direct marketing or mindless harassment, the identification of *likely* neuroblastoma patients who are adduced from the purchased datasets will do the trick. Whether the hypothetical adversary is a pharmaceutical company or

157. *Id.* at 9 (alterations in original).

158. *Id.* at 20 (quoting S. Illinoisan v. Dep't of Pub. Health, 812 N.E.2d 27, 29 (Ill. App. Ct. 2004)).

159. *Id.* at 13.

160. *Id.*

161. *Id.* at 8.

162. More generally, the National Research Council has noted that in cases where "the same data are available elsewhere, even if not in the same form or variable combination, the added risk of releasing a research data file may be comparatively small." COMM. ON NAT'L STATISTICS, NAT'L RESEARCH COUNCIL, IMPROVING ACCESS TO AND CONFIDENTIALITY OF RESEARCH DATA 12 (Christopher Mackie & Norman Bradburn eds., 2000), *available at* http://www.geron.uga.edu/pdfs/BooksOnAging/ConfRes.pdf.

an Erin Brockovich-style environmental torts firm, the adversary could direct its solicitations to the set of likely candidates derived from the purchased, non-anonymized datasets. Dr. Sweeney testified that the requested cancer registry data was the "gold standard" that allowed her to re-identify the patients with confidence,[163] but this overstates the importance of the registry data tables since, without the government's verification, an attacker could still identify the likely candidates with enough confidence for her purposes.

Similarly, Narayanan and Shmatikov overstate the harm that can flow from re-identifying subjects in the Netflix database. Narayanan and Shmatikov explain that their algorithm works best when the movies reviewed on IMDb are less popular films.[164] The authors go into vivid detail in describing the movies that their two re-identified subjects rated in the Netflix database and draw absurd conclusions from them.[165] But they provide no information about the movies that the targets had freely chosen to rate publicly on IMDb using their real names — that is, the information that Narayanan and Shmatikov *already knew* before re-identifying them in the Netflix data. This information is crucial for understanding the marginal utility to putative adversaries. The inferences that are being drawn from the Netflix ratings — that they reveal political affiliation, sexual orientation, or, as the complaint for a recent lawsuit against Netflix alleges, "personal struggles with issues such as domestic violence, adultery, alcoholism, or substance abuse"[166] — can be drawn just as easily from the set of movies that the target had publicly rated in the first place. If the adversary already knows five or six movies that the target has watched, *that* knowledge can go a long way toward pigeonholing and making assumptions about the target.[167]

Of course, it is possible that a public data release could provide a great deal of extra information that would be valuable to a malfeasor.[168] But too often the marginal value is assumed to be very high

---

163. *S. Illinoisan*, 844 N.E.2d at 8.

164. *See* Narayanan & Shmatikov, *supra* note 11, at 116.

165. *Id.* at 123 ("[H]is political orientation may be revealed by his strong opinions about 'Power and Terror: Noam Chomsky in Our Times' and 'Fahrenheit 9/11,' and his religious views by his ratings on 'Jesus of Nazareth' and 'The Gospel of John.'").

166. Doe Complaint, *supra* note 5, at 18.

167. Privacy policy should not aspire to regulate these wrong-headed inferences; plenty of heterosexuals enjoyed Brokeback Mountain, and plenty of liberals dislike Michael Moore. But even if movie reviews are windows to the soul, the marginal information gained by re-identifying somebody in the Netflix dataset is likely to be small.

168. Education datasets often tie non-identifying but highly sensitive information (such as GPA or test scores) to indirect identifiers like age, race, and geography. If individuals in these databases were re-identified using the indirect identifiers, the adversary could learn something significant about the data subjects. *See, e.g.*, Krish Muralidhar & Rathindra Sarathy, *Privacy Violations in Accountability Data Released to the Public by State Educational Agencies*, FED. COMM. ON STAT. METHODOLOGY RES. CONF. 1 (Nov. 2009), http://www.fcsm.gov/09papers/Muralidhar_VI-A.pdf.

without any effort to compare the privacy risks after data release to the risks that exist irrespective of the data release.[169] More to the point, the accretion problem described by Paul Ohm — the prediction that increasing quantities of anonymized data will make re-identification of a rich data profile of us all the more possible[170] — is likely to be overshadowed by the accretion of *identified* data. Given the data mining opportunities available on identifiable information from companies like LexisNexis and Acxiom that aggregate identified information from private insurance and credit companies as well as public records,[171] it is highly unlikely that an adversary will find it worth his time to learn the Shannon entropy formula so that he can apply the Netflix algorithm.

IV. THE SKY IS NOT FALLING: THE REALISTIC RISKS OF PUBLIC DATA

The previous Part provided evidence that the focus of influential computer science literature is preternaturally consumed by hypothetical risks.[172] Unfortunately, legal scholars have taken up the refrain and have come to equally alarmist conclusions about the current state of data sharing.

In considering a public-use dataset's disclosure risk, data archivists focus on marginal risks — that is, the increase in risk of the disclosure of identifiable information compared to the pre-existing risks independent from the data release.[173] Just as the disclosure risk of a data release is never zero, the pre-existing risk to data subjects irrespective of the data release is also never zero. There are always other possible means for the protected information to become public unin-

169. Jeremy Albright, a researcher at the Interuniversity Consortium for Political and Social Research ("ICPSR"), notes that the statistical disclosure control literature has considered this approach but has generally not put it into practice, in part because nobody agrees on how much information the putative adversary should be presumed to have ahead of time. Jeremy Albright, Privacy Protection in Social Science Research: Possibilities and Impossibilities 11–12 (June 1, 2010) (unpublished manuscript) (on file with author).

170. Ohm, *supra* note 4, at 1746.

171. *See* ACXIOM CORP., UNDERSTANDING ACXIOM'S MARKETING PRODUCTS 1 (2010), *available at* http://www.acxiom.com/uploadedFiles/Content/About_Acxiom/Privacy/AC-1255-10%20Acxiom%20Marketing%20Products.pdf; *Risk Solutions Product Index*, LEXISNEXIS, http://www.lexisnexis.com/risk/solutions/product-index.aspx (last visited Dec. 21, 2011).

172. *See, e.g.*, Brickell & Shmatikov, *supra* note 128, at 70 (claiming that "[r]e-identification is a major privacy threat to public datasets containing individual records").

173. NAT'L RESEARCH COUNCIL, *supra* note 162, at 12. Thomas Louis of the University of Minnesota explains that disclosure risks associated with a particular data release should not be compared to a probability of zero, but that one should "consider how the probability of disclosure changes as a result of a specific data release." *Id.* Changes to the marginal risks caused by adding or masking certain fields in the dataset can be assessed as well. *Id.*

tentionally. How much marginal risk does a public research database create in comparison to the background risks we already endure?[174]

This Part assesses the realistic risks posed by the data commons. It lays out the frequency of improper anonymization and analyzes the likelihood that adversaries would choose re-identification as their means to access private information. The unavoidable conclusion is that contemporary privacy risks have little to do with anonymized research data.

A. Defective Anonymization

How often are public datasets released without proper anonymization? In other words, how often do data producers remove direct identifiers only, without taking the additional step of checking for subgroup sizes among indirect identifiers or without consideration to the discoverability of the sampling frame?

Paul Ohm discusses two high-profile examples: Massachusetts hospital data that failed to sufficiently cluster the indirect identifiers, and the AOL search query data that failed to remove last names.[175] This led two journalists at the New York Times to re-identify Thelma Arnold, who shared the spotlight with her search phrase "dog that urinates on everything."[176] Ohm argues that vulnerable public datasets with weak anonymization must be legion.[177] If sophisticated organizations like the Massachusetts Group Insurance Commission and AOL are not getting it right, what could we expect from a local agency?[178]

This concern has merit. A systematic study of disclosures made pursuant to the federal No Child Left Behind Act supports Ohm's in-

---

174. Releases of data by sophisticated data producers are expected, at a minimum, to "assure that the risk of disclosure from the released data when combined with other relevant publicly available data is very low." Working Paper No. 22, *supra* note 109, at 3. Of course, that begs the question what it means for disclosure risk to be "very low." Similarly, "[t]here can be no absolute safeguards against breaches of confidentiality, ... Many methods exist for *lessening* the likelihood of such breaches, the most common and potentially secure of which is anonymity." INT'L STAT. INST., *supra* note 14, at 10. Likewise, the FPCO's commentary on the newly passed FERPA regulations anticipate *low* risk, not the absence of risk altogether. "The regulations recognize that the risk of avoiding the disclosure of PII cannot be completely eliminated and is always a matter of analyzing and balancing risk so that the risk of disclosure is very low." FAMILY POLICY COMPLIANCE ORG., FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT, FINAL RULE, 34 CFR PART 99: SECTION-BY-SECTION ANALYSIS 11 (2008), *available at* http://www.ed.gov/policy/gen/guid/fpco/pdf/ht12-17-08-att.pdf.

175. Ohm, *supra* note 4, at 1717–20; *see also* Nate Anderson, *"Anonymized" Data Really Isn't — And Here's Why Not*, ARS TECHNICA (Sept. 8, 2009, 5:30 AM), http://arstechnica.com/tech-policy/news/2009/09/your-secrets-live-online-in-databases-of-ruin.ars.

176. Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1.

177. Ohm, *supra* note 4, at 1729.

178. *Id.* at 1728.

tuition. The authors, Krish Muralidhar and Rathindra Sarathy, audited publicly available accountability data from several states to see whether the tabulations allow data users to glean PII.[179] While all of the states attempted to implement anonymization protocols, they all got it wrong one way or another.[180] Large repeat players in the data commons like the University of Michigan's Interuniversity Consortium of Policy and Social Research ("ICPSR") or the U.S. Census Bureau do not make these rookie mistakes, and often use data-swapping and noise-adding techniques for an additional level of security.[181] But the data commons no doubt contains some inadequately anonymized datasets that have not undergone best practices. This is almost certainly due to the abysmal state of the guidance provided by regulatory agencies and decisional law. There has not yet been a clear and theoretically sound pronouncement about the steps a data producer should take to reduce the risk of re-identification. I address this problem in Part V. For reasons I will elaborate on now, the risks imposed on data subjects by datasets that do go through adequate anonymization procedures are trivially small.

B. The Probability that Adversaries Exist

The "adversary" or "intruder" from the computer science literature is a mythical creature, the chimera of privacy policy. There is only a single known instance of de-anonymization for a purpose other than the demonstration of privacy risk,[182] and no known instances of a re-identification for the purpose of exploiting or humiliating the data subject. The Census Bureau has not had any known instances of data abuse, nor has the National Center for Education Statistics.[183]

This is not surprising, because the marginal value of the information in a public dataset is usually too low to justify the effort for an intruder. The quantity of information available in the data commons is outpaced by the growth in information self-publicized on the Internet or collected for commercially available consumer data. Consumer

---

179. Muralidhar & Sarathy, *supra* note 168, at 1.

180. *Id.* at 20.

181. RICHARD A. MOORE, JR., U.S. BUREAU OF THE CENSUS, CONTROLLED DATA-SWAPPING TECHNIQUES FOR MASKING PUBLIC USE MICRODATA SETS 25–26, *available at* http://www.census.gov/srd/papers/pdf/rr96-4.pdf.

182. Duff Wilson*, Database on Doctor Discipline is Restored, with Restrictions*, N.Y. TIMES, Nov. 10, 2011, at B2 (News organizations linked identifiable court filings to a national databank of doctor disciplinary actions in order to criticize the disciplinary boards. The journalists re-identified doctors who had a known, long history of malpractice actions against them to the "de-identified" data on disciplinary actions. The public-use data employed trivial anonymization — the removal of names only.).

183. *See* NAT'L RESEARCH COUNCIL, *supra* note 162, at 48; Hermann Habermann, *Ethics, Confidentiality, and Data Dissemination,* 22 J. OF OFFICIAL STAT. 599, 603 (2006).

data catalogs boast that businesses can "choose [an] audience by their ailments & medications."[184]

Unfortunately, privacy advocates routinely fail to report the dearth of known re-identification attacks.[185] Instead, scenarios of re-identification and public humiliation are held up like Desdemona's handkerchief, inspiring suspicion and fear for which we have, as yet, no evidence. As Paul Ohm says,

> Almost every person in the developed world can be linked to at least one fact in a computer database that an adversary could use for blackmail, discrimination, harassment, or financial or identity theft. I mean more than mere embarrassment or inconvenience; I mean legally cognizable harm. Perhaps it is a fact about past conduct, health, or family shame. For almost every one of us, then, we can assume a hypothetical database of ruin, the one containing this fact but until now splintered across dozens of databases on computers around the world, and thus disconnected from our identity. Reidentification has formed the database of ruin and given our worst enemies access to it.[186]

Ohm speaks in the present tense; he suggests the database of ruin has arrived.

It is possible that intruders are keeping their operations clandestine, reverse-engineering our public datasets without detection. But this conviction should not be embraced too quickly. Other forms of data-privacy abuse that ought to be difficult to detect have nevertheless come to light due to whistleblowing and sleuthing.[187] Paul Syver-

---

184. SPECIALISTS MKTG. SERVS., INC., MAILING LIST CATALOG, *available at* http://directdatamailinglists.com/SMS-catalog.pdf.

185. *See, e.g.*, DANIEL SOLOVE, THE DIGITAL PERSON 82–83, 173–74 (2008), *available at* http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text.htm; Ohm, *supra* note 4, at 1729; Brickell & Shmatikov, *supra* note 128, at 70 (claiming that "[r]e-identification is a major privacy threat to public datasets containing individual records"). Thomas M. Lenard and Paul H. Rubin notice this phenomenon, observing that while Solove's study "lists harms associated with information use, he does not quantify how frequent or serious they are." THOMAS M. LENARD & PAUL H. RUBIN, TECH. POLICY INST., IN DEFENSE OF DATA: INFORMATION AND THE COSTS OF PRIVACY 43 (2009), http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf.

186. Ohm, *supra* note 4, at 1748.

187. Pharmatrak, Inc. collected personally identifiable data on web visitors to its pharmaceutical industry clients using clear GIFs (or "cookies") in direct contravention of the Electronic Communications Privacy Act. This practice was exposed and resulted in a class action lawsuit. In re Pharmatrak, Inc., 329 F.3d 9, 12 (1st Cir. 2003). HBGary Federal considered hacking into the networks of its clients' foes in order to gather evidence for smear campaigns, but these practices were uncovered, ironically enough, during a hack into their

son suggests that we could test the hypothesis of covert re-identification by comparing the incidence of identity theft to behaviors or characteristics in accessible datasets to see if there is a correlation that might suggest these data subjects were re-identified at some point.[188] This experiment is worthwhile, but the available aggregate data suggests there is no such relationship. Identity theft plateaued between 2003 and 2009 and dropped to its lowest recorded level in 2010.[189] Moreover, the largest category of identity fraud schemes involves "friendly fraud" — fraudulent impersonation committed by people that know the victim personally (such as a roommate or relative) — and this category has grown in proportion while the other categories declined.[190] These statistics contradict the position that we are inching ever closer to our digital ruination.

Like any default hypothesis, the best starting point for privacy policy is to assume that re-identification does not happen until we have evidence that it does. Because there is lower-hanging fruit for the identity thief and the behavioral marketer — blog posts to be scraped and consumer databases to be purchased — the thought that these personae non gratae are performing sophisticated de-anonymization algorithms is implausible.

C. Scale of the Risk of Re-Identification in Comparison to Other Tolerated Risks

Privacy risks are difficult to measure and understand — to feel at a gut level.[191] One useful heuristic for comprehending the privacy risks of public anonymized data is to compare those risks to other privacy risks that we know and tolerate.

Our trash is a rich and highly accessible source of private information about us — indeed, it continues to have the distinction of being a tremendously valuable resource for private investigators and

---

own servers. *See* Eric Lipton & Charlie Savage, *Hackers' Clash with Security Firm Spotlights Inquiries to Discredit Rivals*, N.Y. TIMES, Feb. 11, 2011, at A15.

188. Paul Syverson, *The Paradoxical Value of Privacy*, 2D ANN. WORKSHOP ON ECON. & INFO. SECURITY 2 (2003), http://www.cpppe.umd.edu/rhsmith3/papers/Final_session3_syverson.pdf.

189. *The Notable Decline of Identity Fraud*, HELP NET SECURITY (Feb. 8, 2011), www.net-security.org/secworld.php?id=10551; *see also* LENARD & RUBIN, *supra* note 185, at 34–35. The aggregate data cannot directly answer the question about the relationship between public data and identity theft. Ironically, microdata is required to reliably test this theory of covert re-identification.

190. *See The Notable Decline of Identity Fraud*, *supra* note 189.

191. This is at the heart of Peter Swire's criticism of scholars like me who attempt to compare the costs and benefits of privacy. *See* Peter Swire, Privacy and the Use of Cost/Benefit Analysis 4, 10 (June 18, 2003) (unpublished manuscript), *available at* http://www.ftc.gov/bcp/workshops/infoflows/present/swire.pdf.

identity thieves.[192] Data presents no more risk (and often less risk) than our garbage. Thomas Lenard and Paul Rubin have noted that breach notification requirements and other warnings about the privacy hazards of conducting business online could lead consumers to conduct business offline and demand paper statements. Ironically, this result would greatly increase the likelihood of identity theft.[193]

Moreover, consider the large quantity of sensitive personally identifiable information available in public records. Income information, thought to be among the most sensitive categories of information,[194] is available for most public employees.[195] The names and salaries of the highest-paid employees in California are tracked on the Sacramento Bee's website.[196] Litigants and witnesses in lawsuits are often forced to divulge personal information and face embarrassing accusations, and juror identities and questionnaire responses are usually within the public domain.[197] We accept these types of exposures because the countervailing interests — ensuring transparency and accountability in state action — warrant it. The Constitution protects these types of disclosures through a robust set of First Amendment precedents, and the tradeoffs in terms of privacy invasions have proven to be bearable to society.[198]

The closest cousin to the malicious de-anonymizer is the hacker. This type of adversary certainly exists. If we are to imagine a skilled computer programmer determined to find out a target's secrets, is it not easier to imagine him just hacking into the target's personal computer? This, after all, was HBGary Federal's modus operandi when it consulted to do the dirty work for Bank of America, corporate law firms, and their clients.[199] HBGary Federal planned to create extensive dossiers of rivals or critics for the purpose of forming smear campaigns.[200] When HBGary Federal proposed to make a dossier on members of U.S. Chamber Watch, a consumer watchdog organiza-

---

192. Frank Abagnale stresses the importance of eliminating the garbage and paper trail to reduce the risk of identity fraud. *See Abagnale Recommends Fraud Protection Strategy: Audio*, BLOOMBERG (Nov. 15, 2010), http://www.bloomberg.com/news/2010-11-15/abagnale-recommends-fraud-protection-strategy-audio.html.

193. LENARD & RUBIN, *supra* note 185, at 38–39.

194. *See* Bernardo A. Huberman, Eytan Adar & Leslie R. Fine, *Valuating Privacy*, IEEE SECURITY & PRIVACY, Sept.–Oct. 2005, at 22, 22–24.

195. For example, see the salary information available online for University of Michigan employees at http://www.umsalary.info/deptsearch.php.

196. *State Worker Salary Search: Top Salaries Earned in 2010*, THE SACRAMENTO BEE, http://www.sacbee.com/statepay (last visited Dec. 21, 2011); *see also* Comm'n on Peace Officer Standards and Training v. Superior Court, 165 P.3d 462, 465 (Cal. 2007).

197. *See, e.g.*, Pantos v. City & Cnty. of S.F., 198 Cal. Rptr. 489, 491 (Cal. Ct. App. 1984); Forum Commc'ns Co. v. Paulson, 752 N.W.2d 177, 185 (N.D. 2008).

198. *See* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 496 (1975); Fla. Star v. B.J.F., 491 U.S. 524, 538 (1989).

199. Lipton & Savage, *supra* note 187.

200. *Id.*

tion, their plans included identifying vulnerabilities in the targets' computer networks that could be exploited.[201] HBGary Federal responded to the incentives to engage in unethical and illegal behavior to garner the favor of its clients. Yet, it is difficult to imagine that HBGary's agenda would ever include re-identifying their targets in public-use anonymized datasets. The alternative approaches are so much easier.

A malfeasor with no specific target in mind is still better off using hacking techniques rather than de-anonymization algorithms. That is what hackers did to expose 236,000 mammography patient records at the University of North Carolina School of Medicine,[202] 160,000 health records for University of California students,[203] and 8,000,000 records in the Virginia Prescription Monitoring Program (for which the hackers sought a $10 million ransom).[204] These sorts of hacks require significantly less skill than the de-anonymization of a research dataset because malware capable of exploiting bugs in popular programs and operating systems is sold on the black market to whomever is unethical enough to use it.[205] The programs require little to no customization because they apply malicious code to popular programs that all suffer from identical vulnerabilities.[206] De-anonymization algorithms, in contrast, require a theoretical understanding of the algorithm in order to suit the attack to a particular dataset.[207]

Data spills — the mishandling of unencrypted data — provide another illustration of the risk of re-identification. These spills typically expose the personally identifiable information of customers or patients. In the last couple years the medical records of 7.8 million people have been exposed in various sorts of security breaches.[208] The

---

201. *Id.* Ironically, it was HBGary Federal's own networks' vulnerabilities that it should have been focusing on, as the hacker group Anonymous hacked into HBGary Federal's servers and released several emails and PowerPoint presentations on Wikileaks. *Id.*

202. *Hackers Attack UNC-Based Mammography Database,* UNC HEALTH CARE (Sept. 25, 2009), http://news.unchealthcare.org/som-vital-signs/archives/vital-signs-sept-25-2009/hackers-attack-unc-based-mammography-database.

203. *Hackers Get Into U.C. Berkeley Health-Records Database*, FOXNEWS.COM (May 8, 2009), http://www.foxnews.com/story/0,2933,519550,00.html.

204. Brian Krebs, *Hackers Break into Virginia Health Professions Database, Demand Ransom*, WASH. POST SECURITY FIX (May 4, 2009, 6:39 PM), http://voices.washingtonpost.com/securityfix/2009/05/hackers_break_into_virginia_he.html.

205. *See* Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1101 (2011); *see also* Larry Barrett, *Data Theft Trojans, Black Market Cybercrime Tools on the Rise*, ESECURITY PLANET (Mar. 31, 2010), http://www.esecurityplanet.com/trends/article.php/3873891/Data-Theft-Trojans-Black-Market-Cybercrime-Tools-on-the-Rise.htm.

206. *See* Bambauer & Day, *supra* note 205, at 1060–62; Jaziar Radianti & Jose J. Gonzalez, Toward a Dynamic Modeling of the Vulnerability Black Market 4–7 (Oct. 23–24, 2006) (unpublished manuscript), *available at* http://wesii.econinfosec.org/draft.php?paper_id=44.

207. *See supra* Part III.

208. Milt Freudenheim, *A New Push to Protect Health Data*, N.Y. TIMES, May 31, 2011, at B1.

spills are often the result of improper handling by employees who were authorized to access the information. For example, Massachusetts General Hospital recently agreed to pay a one million dollar fine after one of its employees lost the records of 192 patients on the subway, many of whom had HIV/AIDS.[209] So the question for our purposes is this: if we are to fear users of public anonymized datasets, why do we tolerate the handling of our personal information by minimally paid, unskilled data processors?[210] (Indeed, some companies have used prison labor to perform data entry.[211])

The intuitive answer is that data has become the lifeblood of our economy. It is more rational to spread risk among all the consumers and modify data handling behavior through fines and sanctions than it is to expect consumers to forego the convenience and customized service of the information economy.[212] It is puzzling, then, why privacy advocates have chosen to target anonymized research data — data that poses relatively low risk to the citizenry and offers valuable public-interest-motivated research in return — as a cause worthy of preemptive strike.[213]

V. A PROPOSAL IN THE STATE OF HIGHLY UNLIKELY RISK

The fractured set of privacy statutes and rules in the United States generally requires data producers to refrain from releasing data that can be used to re-identify a data subject.[214] A great limitation of current U.S. privacy law — a limitation that runs against the interests of the data subjects and researchers alike — is that privacy law regulates

209. *See Morning Edition: MGH Settles for $1M over Lost HIV/AIDS Records*, NAT'L PUB. RADIO (Feb. 25, 2011), http://www.wbur.org/2011/02/25/mgh-privacy.

210. In Massachusetts General Hospital's case, the employee was a billing manager, and not a low skilled employee. *Id.* But records, particularly consumer records, are often in the hands of low skill data processors or outsourced to third parties that process the data offshore. *See, e.g.*, *Outsourcing Data Entry Privacy Policy*, DATA ENTRY SERVICES INDIA, http://www.dataentryservices.co.in/privacy_policy.htm (last visited Dec. 21, 2011). Not everybody is comfortable with the risk that accompanies routine data-handling. Parents of a student who participated in a research survey at their child's school attempted to mount a legal challenge based on the potential privacy risks that an administrator might divulge their child's information inadvertently, but the suit was dismissed. C.N. v. Ridgewood Bd. of Educ., 430 F.3d 159, 161 (3d Cir. 2005).

211. Sandra T.M. Chong, *Data Privacy: The Use of Prisoners for Processing Personal Information*, 32 U.C. DAVIS L. REV. 201, 204 (1998).

212. *See* Cate, *supra* note 9, at 12–16. Poor encryption practices are an excellent target for effective privacy regulation. There is no reason for a business or agency to fail to encrypt its files that contain personally identifiable information. *See* Derek E. Bambauer, *Rules, Standards, and Geeks*, 5 BROOK. J. CORP. FIN. & COM. L. 49, 56–57 (2010).

213. A wiser target is the law surrounding data security breaches. *See, e.g.*, Paul M. Schwartz and Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007); *see also* Bambauer, *supra* note 212, at 49.

214. *See supra* text accompanying notes 20–21.

the *release* of data rather than its use.[215] Privacy law does not prohibit an end-user from re-identifying somebody in a public-use dataset. Rather, the laws and statutory schemes act exclusively on the releaser.[216] In many respects, the current approach to data privacy is dissatisfying to the full range of affected parties, and we are beginning to see an influx of new proposals.

The most popular suggestions for altering data privacy laws differ in their particulars, but they invariably impose large transaction costs on research, if they do not preclude it altogether. The FTC's recently unveiled framework for consumer data advises companies not to distinguish between anonymized and personally identifiable data, which means that anonymized research data must be subjected to the exact same limitations imposed on the collection and use of identifiable data.[217] This vision bars private companies from participating in the data commons, since a public release of research data would be treated the same as a security breach or a spill of identifiable data. The FTC's framework borrows from the European Data Protection Directive, which requires the unambiguous consent of data subjects before personal data can be processed into statistical research data.[218] If the FTC framework is a harbinger for what is to come, the data commons is in real trouble.[219]

Paul Ohm and Daniel Solove propose "contextual" privacy regulations to bring legal liability in line with the risk that the data producer has created.[220] Ohm suggests that a data releaser should consider all the determinants of re-identification risk and assess whether a threat to the data subject exists.[221] While this solution has natural appeal as a levelheaded approach, a loose case-by-case standard will provide little guidance and assurance for data producers. In fact, existing statutes already implement the bulk of the suggestions Ohm puts forward. HIPAA regulations, for example, instruct data producers to remove

---

215. *Id.*

216. *Id.*

217. FTC PRIVACY REPORT, *supra* note 5, at 43, 51–52.

218. *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2001 O.J. (L 281) 31, 34, 40. Note that under Recital 29, processing for statistical purposes is, at least, not a use inconsistent with any other use for which the data may be processed. *Id.* at 34. Social science researchers often have to perform their analyses at the physical location of the data enclaves. *See, e.g.*, Stefan Bender et al., *Improvement of Access to Data Set from the Official Statistics* 4–5 (German Council for Soc. and Econ. Data, Working Paper No. 118, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1462086.

219. Legislation seeking to limit the storage of data has already been proposed. *See, e.g.*, Eliminate Warehousing of Consumer Internet Data Act of 2006, H.R. 4731, 109th Cong. (2006).

220. Ohm, *supra* note 4, at 1762; Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1091–93 (2002).

221. Ohm, *supra* note 4, at 1764.

any information that, in context, might lead to the re-identification of a data subject, and they differentially scrutinize public releases much more severely, while giving agencies and firms wide latitude when drawing up licenses with business associates.[222] But for the reasons detailed in Part II, these standards are encouraging over-protectionism and providing agencies with an evasion tactic. Moreover, licensing processes impose transaction costs on researchers that are not justified by the speculative risks of re-identification.

I propose something altogether different: simple, easy-to-apply rules.[223] My policy has three aspects to its design: (1) it clarifies what a data producer is expected to do in order to anonymize a dataset and avoid the dissemination of legally cognizable PII; (2) it immunizes the data producer from privacy-related liability if the anonymization protocols are properly implemented; and (3) it punishes with harsh criminal penalties any recipient of anonymized data who re-identifies a subject in the dataset for an improper purpose. I will describe each of these aspects in more detail and explain why the proposed approach offers an improvement over current laws and regulations.

A. Anonymizing Data

Under my approach, a data producer is required to do just two things in order to convert personally identifiable data into anonymized (non-PII) data: (1) strip all direct identifiers, and (2) either check for minimum subgroup sizes on a preset list of common indirect identifiers — such as race, sex, geographic indicators, and other indirect identifiers commonly found in public records — or use an effective random sampling frame.

(1) *Stripping Direct Identifiers.* The removal of direct identifiers (name, telephone number, address, social security number, IP addresses, biometric identifiers like fingerprints, and any other unique identifying descriptor) is an obvious first step, but one that should not go without comment. After all, this critical oversight led to the re-

222. For instance, under HIPAA, the public release of health information requires the covered entity to prepare the data such that "there is no reasonable basis to believe that the information can be used to identify an individual." 45 C.F.R. § 164.514(a) (2010). Releases of identifiable health information to a business associate, on the other hand, are permitted so long as the business associate makes assurances that it will guard and handle the health data in a manner consistent with the covered entity's responsibilities under HIPAA. *Id.* § 164.502(e)(1)(i) (2010). Any additional restrictions the covered entity might wish to impose are left to the original data-holder's discretion.

223. Derek Bambauer argues that rules are more helpful than standards in contexts when three conditions are met: (1) when the specified minimum standard for behavior will suffice most or all of the time, (2) when the standard degrades slowly, and (3) when monitoring for harm is low-cost and accurate. Bambauer, *supra* note 212, at 50. Here, the first condition is met because, as I argued earlier, re-identificaiton attacks performed on anonymized data are difficult, and anonymization has sufficed to prevent re-identification attacks. *See supra* Parts III, IV. The second and third conditions are developed in this Part.

identification of a data subject in the AOL search term database.[224] Remarkably, the privacy community and even the FTC have held this up as a key exemplar for the proposition that there is no viable way to adequately anonymize data anymore.[225] In fact, the AOL story is an example of a *lack* of anonymization.

(2) *Basic Risk Assessment.* My next step requires the data producer either to count the *minimum subgroup sizes* or to confirm that the dataset has an *unknown sampling frame*. Neither of these is conceptually difficult.

Minimum Subgroup Count — This ensures that no combination of indirect identifiers yields fewer than a certain threshold number of observations (usually between three and ten). For the purpose of this Article I will use five.[226] This is known as "k-anonymity" in the computer science literature.[227] Suppose a college wishes to release a public-use version of its grades database. If there are only two Asian female chemistry majors in the cohort of students that entered in 2010, then the school should not release a dataset that includes race, gender, major, and cohort year unless it first blurs together some of these categories. The college might choose to lump several majors together into clusters, or lump cohort years into bands spanning five years. There are a number of ways to blur the categories such that minimum subgroup counts stay above the required threshold. Indirect identifiers are limited to categories of information that are publicly available for all or most of the data subjects — e.g., age, gender, race, and geographic location. They do not include information that is not systematically compiled and distributed by third parties.[228]

Unknown Sampling Frame — If a public data user has no basis for knowing whether an individual is in the universe of people described in the dataset, then the dataset does not — and cannot — disclose PII. Sampling frame is a powerful tool for anonymizing data, and large statistical bureaus (such as the U.S. Census Bureau) often employ it when they collect information on a random sample of

224. AOL failed to strip the dataset of last names. This oversight, in combination with multiple searches for a particular neighborhood, led to the re-identification of Thelma Arnold. Barbaro & Zeller, *supra* note 176.

225. FTC PRIVACY REPORT, *supra* note 5, at 36, 38. The AOL story, along with the Netflix study, was the support for the FTC's broad-reaching conclusion that "businesses combine disparate bits of 'anonymous' consumer data from numerous different online and offline sources into profiles that can be linked to a specific person." *Id.*

226. The Centers for Disease Control and Prevention anticipates aggregated tables using a threshold value of three. CTRS. FOR DISEASE CONTROL AND PREVENTION & HEALTH RES. SERVS. ADMIN., INTEGRATED GUIDELINES FOR DEVELOPING EPIDEMIOLOGIC PROFILES 126 (2004), *available at* http://www.cdc.gov/hiv/topics/surveillance/resources/guidelines/epi-guideline/pdf/epi_guidelines.pdf.

227. *See* Sweeney, *supra* note 18, at 557.

228. For example consumer preferences and information contained on a Facebook "wall" are not indirect identifiers in my scheme.

Americans.[229] Thus, if the Bureau of Labor Statistics produces a dataset that includes only one veterinarian in Delaware, we need not be concerned unless there is some way to know which of the many veterinarians in Delaware the dataset is describing. If the sampling frame is unknown, then the minimum subgroup count and extremity-coding rules need not apply.[230] But precautions must be taken to ensure that an outsider really cannot discern whether the sample includes a particular individual.[231]

If either of these protocols is properly implemented, the dataset would be legally recognized as anonymized non-PII data. To be clear, this standard is *less* onerous than the current state and federal laws like HIPAA. This is by design. While my proposal diverges sharply from others', it flows naturally from the assertion, supported earlier in this Article, that the risk of re-identification is not significant. Nevertheless, agencies and organizations that work with data frequently enough to have Institutional Review Boards should continue to use heightened standards determined by current best practices.[232] The procedures described above set an appropriate floor, and need not be interpreted as a ceiling.

Freeing up the flow of data will enrich the proverbial marketplace of ideas. In the past, the simplified process of stripping obvious identifiers was legally sufficient to protect an individual's privacy.[233] We have drifted into protecting against more and more intricate attacks without having experienced any of them. Moreover, some of the more complex disclosure-risk avoidance techniques (such as data-swapping or noise-adding) have gone awry. The U.S. Census Bureau's public-use microdata samples ("PUMS files") from the 2000 census contain

---

229. For example, the Public-Use Microdata Samples ("PUMS files") report data on a sample of U.S. households. *See Public-Use Microdata Samples (PUMS)*, U.S. CENSUS BUREAU, http://www.census.gov/main/www/pums.html (last updated May 28, 2010).

230. This assumption can fail in circumstances where a potential data subject is unusual. If the indirect identifiers included in the dataset uniquely describe a person in the broad population of people that could potentially be included in the sample, an adversary will be able to check whether that person actually *is* included in the sample (and identify him if he is). For example, suppose only one veterinarian in Delaware identifies himself as a Native American; a dataset that included profession, state, and detailed race information cannot rely on an unknown sampling frame to ensure anonymity because any dataset including these indirect identifiers would immediately identify the individual in question as being a member of the dataset.

231. *See, e.g.*, Khaled El Emam & Fida Kamal Dankar, *Protecting Privacy Using k-Anonymity*, 15 J. AM. MED. INFO. ASS'N 627, 634–35 (2008).

232. *See* George T. Duncan, *Confidentiality and Data Access Issues for Institutional Review Boards*, *in* PROTECTING PARTICIPANTS AND FACILITATING SOCIAL AND BEHAVIORAL SCIENCES RESEARCH 235, 235 (Constance F. Citro et al. eds., 2003).

233. *See* Nat'l Cable Television Ass'n v. FCC, 479 F.2d 183, 195 (D.C. Cir. 1973); Tax Analysts and Advocates v. IRS, 362 F. Supp. 1298, 1307 (D.D.C. 1973) (quoting *Nat'l Cable Television Ass'n*, 479 F.2d at 195)

substantial errors in the reporting of age and gender that have affected analyses for a decade's worth of research.[234]

B. Safe Harbor for Anonymized Data

If a data producer follows the anonymization protocols, it will be shielded from liability based on privacy torts, certain types of contractual liability, and federal statutory penalties defined by privacy statutes like HIPAA. The anonymization protocols would also take the data out of the ambit of privacy exemptions in public records statutes (meaning that government agencies legally obligated to disclose information through public records laws could not make use of the privacy exemption if a useful dataset could be produced using the anonymization procedures described above). With the exception of contractual liability, on which I elaborate below, the scope of this safe harbor provision is fairly predictable.

The safe harbor provision protects data producers from liability based on confidentiality agreements unless the confidentiality agreement explicitly prohibits the dissemination of all information, whether or not it is in identifiable form, to any unnamed third parties. To be clear, if the firm collecting data reserves the right to share information to a third party in the private agreement, anonymized data will not violate the confidentiality agreement. The reason for structuring the safe harbor provision this way is to prevent the very likely scenario in which a company wishes to profit from the information it collects by sharing it with marketers or business partners, while simultaneously having a consumer-friendly-sounding excuse for shielding anonymized data from researchers who might use the data to uncover fraud or discrimination. Of course, nothing in this scheme obligates an organization to share anonymized research data, but it does remove the fig leaf — the pretense of sensitivity — when data is shared for marketing and business purposes.

Immunity is bold, but it is not unusual for the law to go to great lengths to bolster the public's interest in information. Courts have been especially protective of the First Amendment right to disseminate truthful information of public concern.[235] In the context of undercover journalism, scholars and lawmakers have concluded that the public interest in unearthing information justifies immunity from tort liability, even when journalists employ deceptive newsgathering prac-

---

234. *See* J. Trent Alexander, Michael Davern & Betsey Stevenson, *Inaccurate Age and Sex Data in Census PUMS Files* 1–3 (CESifo Working Paper No. 2929, 2010), *available at* http://ssrn.com/abstract=1546969; Steven Levitt, *Can You Trust Census Data?*, FREAKONOMICS (Feb. 2, 2010, 11:09 AM), http://www.freakonomics.com/2010/02/02/can-you-trust-census-data.

235. *See* Bartnicki v. Vopper, 532 U.S. 514, 515, 518 (2001); Fla. Star v. B.J.F., 491 U.S. 524, 525 (1989); Sidis v. F-R Publ'g Corp., 113 F.2d 806, 807–09 (2d Cir. 1940).

tices.[236] C. Thomas Dienes notes that "[i]n the private sector, when the government fails in its responsibility to protect the public against fraudulent and unethical business and professional practices, whether because of lack of resources or unwillingness, media exposure of such practices can and often does provide the spur forcing government action."[237] Likewise, Erwin Chemerinsky defends paparazzi-style journalism by reminding the academy:

> Speech is protected because it matters in people's lives, and aggressive newsgathering is often crucial to obtaining the information. The very notion of a marketplace of ideas rests on the availability of information. . . . People on their own cannot expose unhealthy practices in supermarkets or fraud by telemarketers or unnecessary surgery by doctors. But the media can expose this, if it is allowed the tools to do so, and the public directly benefits from the reporting.[238]

Undeniably, the data commons is one of these tools. It provides invaluable probative power that cannot be matched by anecdote or concentrated theorizing, and the risk of re-identification is relatively small compared to the informational value.

C. Criminal Penalties for Data Abuse

Finally, the safe harbor must be buttressed by a statute that criminalizes and stiffly punishes the improper re-identification of subjects within a properly anonymized dataset.[239] Criminal liability attaches the instant an adversary discloses the identity and a piece of non-public information to one other person who is not the data producer.[240] First, this design avoids unintentionally criminalizing disclosure-risk research — research that can usefully identify vulnerabilities in anonymized datasets. This sort of information will be invaluable to

---

236. *See* Desnick v. ABC, 44 F.3d 1345, 1354–55 (7th Cir. 1995); Erwin Chemerinsky, *Protect the Press: A First Amendment Standard for Safeguarding Aggressive Newsgathering*, 33 U. RICH. L. REV. 1143, 1160 (2000). *But see* Food Lion, Inc. v. ABC, 194 F.3d 505, 521 (4th Cir. 1999).

237. C. Thomas Dienes, *Protecting Investigative Journalism*, 67 GEO. WASH. L. REV. 1139, 1143 (1999).

238. Chemerinsky, *supra* note 236, at 1160.

239. In order to trigger criminal protection against re-identification, the dataset must be properly anonymized in accordance with the requirements affording safe harbor protection. This prevents users of a poorly anonymized dataset from incurring criminal liability.

240. If the sample frame is unknown, non-public information can consist of information reported about the subject in the dataset or even the mere fact that the subject is in the dataset.

data producers and regulators if an attack seems likely to be replicated by a true malfeasor. De-anonymization scientists will be able to continue publishing their work with impunity. Second, this design avoids the possibility of innocent technical violations by requiring an overt, malicious act — disclosing a non-public piece of information to one other person.[241]

Current privacy statutes leave a blatant gap in coverage: they do not restrain an adversary from re-identifying a subject. To address this, the Institute of Medicine of the National Academies has proposed legal sanctions for re-identification,[242] and Robert Gellman has proposed a system of data sharing through uniform licensing agreements that protect against the re-identification of data subjects using criminal and civil sanctions.[243] In fact, much of the public research data available to researchers today requires the execution of data license agreements prohibiting re-identification and requiring the research staff to ensure the security of the data.[244] A federal criminal statute would provide uniform protection for all data subjects, and would reduce transaction costs between data users and data producers by making contractual promises of this sort unnecessary.

The criminal penalty is particularly important when a dataset has been properly anonymized, but an adversary decides to target a specific data subject about whom the adversary has special information. Take the following example, which comes from the Department of Education's commentary on the 2009 revisions of the FERPA regulations:

> [I]f it is generally known in the school community that a particular student is HIV-positive . . . then the school could not reveal that the only HIV-positive student in the school was suspended. However, if it

241. I do not believe this precaution is necessary to avoid "thought crimes." After all, tort law has made actionable some forms of observation in public. For example, even mere public surveillance can be actionable under the tort of intrusion. *See* Summers v. Bailey, 55 F.3d 1564, 1566 (11th Cir. 1995); Nader v. Gen. Motors Corp., 255 N.E.2d 765, 769–71 (N.Y. 1970). The reverse-engineering of an anonymized dataset is at least as intrusive and requires just as much actus reus.

242. INST. OF MED. OF THE NAT'L ACADS., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 265 (Sharyl J. Nass et al. eds., 2009), *available at* http://www.ncbi.nlm.nih.gov/books/NBK9578/pdf/TOC.pdf.

243. Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33, 51–52 (2010). Paul Ohm also suggests that regulators should consider prescribing "new sanctions — possibly even criminal punishment — for those who reidentify." Ohm, *supra* note 4, at 1770. Both Gellman's and the Institute of Medicine's proposals restrict researchers from sharing the de-identified data outside their research teams. Gellman, *supra*, at 51–52; INST. OF MED. OF THE NAT'L ACADS., *supra* note 242, at 49–50. My proposal does not prohibit re-disclosure of anonymized data.

244. *See, e.g.*, *Restricted Data Use Agreement*, ICPSR, http://www.icpsr.umich.edu/icpsrweb/ICPSR/access/restricted/agreement.jsp (last visited Dec. 21, 2011).

> is not generally known or obvious that there is an HIV-positive student in school, then the same information could be released, even though someone with special knowledge of the student's status as HIV-positive would be able to identify the student and learn that he or she had been suspended.[245]

Likewise, someone with special knowledge about the circumstances of a particular student's suspension could use that information to discern that he or she is HIV-positive. While the student might have civil recourse if the adversary publicizes this fact and causes sufficient harm,[246] nothing in FERPA's design outlaws the adversary's acts in re-identifying the student in the first place. The heavy hand of the prosecutor is an appropriate means for enforcing the ethics of the data commons.

Though detection and enforcement of this provision would no doubt be very difficult, this does not mean that retributive disincentives have no effect. People and firms often overreact to improbable but unknown risks of criminal sanction.[247] Moreover, one major motivation for my proposal is the understanding that re-identification is unlikely to happen. Thus, the criminal element to this data privacy scheme is, by design, expensive and likely to operate more as a disincentive than as a penalty actually imposed by courts.

D. Objections

The objection to my framework is simple: What if I am wrong? By the time we realize that anonymization can be undone, it is too late! Ohm's contention is that data that cannot re-identify us today will be capable of doing so tomorrow.[248] We need urgent action because we are laying the groundwork for the "database of ruin."[249] This argument shares a remarkable resemblance to fears about the introduction of computers into the federal government in the 1960s. The statement of Representative Cornelius E. Gallagher of New Jersey before the Committee on Government Operations is typical of these fears:

---

245. Family Educational Rights and Privacy, 73 Fed. Reg. 74,806, 74,832 (Dec. 9, 2008).

246. The student might be able to bring a claim based on the tort of public disclosure of private facts. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

247. *See* John E. Calfee & Richard Craswell, *Some Effects of Uncertainty on Compliance with Legal Standards*, 70 VA. L. REV. 965, 966 (1984). This reaction is also reflected in the high prices firms pay for criminal liability insurance. *See* Miriam H. Baer, *Insuring Corporate Crime*, 83 IND. L.J. 1035, 1036 (2008).

248. Ohm, *supra* note 4, at 1748, 1757.

249. *Id.* at 1757.

> Nor do we wish to see a composite picture of an individual recorded in a single informational warehouse, where the touch of a button would assemble all the governmental information about the person since his birth. . . . Although the personal data bank apparently has not been proposed as yet, many people view this proposal as a first step toward its creation. . . . We cannot be certain that such dossiers would always be used by benevolent people for benevolent purposes.[250]

Anxieties over potential abuse of new information technologies are a hardy perennial.[251] Today, the threatening technology is the Internet. While the Internet certainly increases the risk of re-identification, and while producers of anonymized data should be cognizant of new and rich collections of auxiliary information available to a malicious intruder, the additional risk is not as great as it might seem. Remember that, in order to re-identify a subject in a dataset, an adversary must be confident that a unique data subject matches a unique member of the general population.[252] Suppose an anonymized prescription dataset described a fifty-year-old woman in central Vermont who is taking pharmaceutical drugs to treat depression and high cholesterol. An adversary comes across a LiveJournal blog post by a woman who identifies herself, reveals that she is fifty years old and living in Montpelier, and describes her experience on Lipitor.[253] The adversary has stumbled upon a likely candidate to match up to the anonymized data subject, and if he is right, he will have learned that the blogger is also clinically depressed. But in order to be confident in the match, he must have some reason to believe that this is the *only* fifty-year-old woman in central Vermont using a cho-

250. *The Computer and Invasion of Privacy: Hearings Before a Subcomm. of the Comm. on Gov't Operations*, 89th Cong. 3 (July 26–28, 1966).

251. The congressional hearings in the late 1960s led to the passage of the Privacy Act of 1974. *The Privacy Act of 1974*, EPIC, http://epic.org/privacy/1974act (last visited Dec. 21, 2011) [hereinafter *EPIC Privacy Act Report*]. This law bars government agencies from collecting, sharing, and retaining information that is not necessary for carrying out official duties. 5 U.S.C. § 552a(b) (2006). But the Privacy Act is the result of an odd collection of compromises, *EPIC Privacy Act Report*, *supra*, so its ability to protect against the creation of data profiles is limited. It contains a number of exceptions, including the routine use exemption (which is arguably the exception that swallows the rule), *id.* § 552a(b)(3), and exceptions for law enforcement investigations, *id.* § 552a(b)(7). For a criticism of the routine use exemption, see Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 584–87 (1995), and Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 198 (Philip E. Agre & Marc Rotenberg eds., 1997).

252. *See supra* Part III.

253. This example comes from a dissenting opinion from a recent medical privacy lawsuit. *See* IMS Health Inc. v. Sorrell, 630 F.3d 263, 283 (2d Cir. 2010) (Livingston, J., dissenting), *aff'd*, 131 S. Ct. 2653 (2011).

lesterol-lowering drug. The Internet provides a lot of information about a lot of people, but it is not a source of comprehensive and systematic information, so it is a flawed tool for the malicious intruder. At best, the adversary might be able to use some statistical source of medical treatment rates to estimate the likelihood that the Montpelier woman is unique.

Ohm and other critics of anonymization believe that once adversaries are able to sync up one anonymized database to identities, they will be able to match the combined database to a third anonymous database, and then a fourth, et cetera, until a complete profile is built.[254] This threat is premised on perfect matching attacks that contain no false matching error. If a re-identification attack is assumed to have error (which it most certainly will in the absence of a complete population registry of some sort), then the quality of the dossier will be so poor as to undermine its threat. Even in the unlikely scenario where each re-identification attack contains only a ten percent false match rate, twenty-seven percent of the observations in the combined dataset will likely contain errors.[255]

Even ignoring the snowballing error rates, the value to an adversary of anonymized data erodes over time. If adversaries are able and willing to make entropic re-identification attacks in the future, anonymized data from today will have vanishing value as time trots on for two reasons. First, people's attributes change, so making matches will be increasingly hard and subject to false positives and false negatives. Studies on databases that are known to cover the same population are, in fact, frequently difficult to match up because the subject's contemporaneous responses to the same or similar questions are often incompatible.[256] And since the profiles used to make the match will likely be riddled with error, matching to old data will often fail.[257] Second, even if a successful match is made and is verifiable, there will be less intrinsic value to knowing old attributes. No matter what the adversary's bad motives are, the value of old data (again, its marginal utility) decreases with time.

---

254. *See* Ohm, *supra* note 4, at 1725–27. Likewise, EPIC has the same conviction, claiming that the harms caused by the release of the (non-)anonymized AOL search query data will increase over time since re-identifying more AOL subjects will be easier as more and more data enters the public domain. *See Re-identification*, *supra* note 5.

255. $(0.9)^3 = 0.73$. And, of course, the adversary will not know which twenty-seven percent of entries contain the expected errors.

256. Müller, et al., *supra* note 127.

257. Even commercial data aggregation, which has the luxury of linking *identified* information, is riddled with error. Joel Stein documented the false information in his own commercial profiles in a recent *Time* article. Joel Stein, *Your Data, Yourself*, TIME, Mar. 21, 2011, at 40. Though the profiles are useful for advertising purposes, they suggest that a "database of ruin" is a fantasy well out of reach. One of the commercial databases believed that Joel Stein was an eighteen- to nineteen-year-old woman. *Id.*

Privacy advocates tend to take on the role of doom prophets — their predictions of troubles are ahead of their time.[258] Convinced of the inevitability of the harms, privacy scholars are dissatisfied with reactive or adaptive regulation and insist on taking prospective, preemptive action.[259] Dull as it is, reactive legislation is the most appropriate course for anonymized research data. Legislation inhibiting the dissemination of research data would have guaranteed drawbacks today for the research community and for society at large. We should find out whether re-identification risk materializes before taking such drastic measures.

E. Improving the Status Quo

In the meantime, we would do well to clean up the muddled state of the PII-based privacy system currently in place. Right now case law and regulatory guidance are so reluctant to commit to a protocol that data producers cannot be sure what is expected of them.

The regulatory goal of a PII-based privacy statute is quite straightforward: a data user should not be able to learn something new about a data subject using publicly available auxiliary information. Direct identifiers are removed, of course, and some additional precautions are often required. The mandates of current privacy statutes can be met using what I will refer to as the "Four Key Principles" of PII-based anonymization. These principles are not beyond the capabilities of a FOIA officer at a public agency:

(1) *Unknown Sampling Frame* — If the data producer is confident that data users cannot use public information to determine whether somebody is in the dataset or not, the other precautions described in this section need not be taken.[260]

(2) *Minimum Subgroup Count* — This concept is incorporated into my proposal above: the data producer ensures that no combination of indirect identifiers yields fewer than a certain threshold number of observations. The data producer must use good judgment in categorizing the variables as indirect identifiers or non-identifiers.[261]

---

258. Occasionally this kind of prediction is accomplished by reminiscing about simpler times. Jeffrey Rosen, for example, believes the Internet compares unfavorably to the villages described in the Babylonian Talmud. Jeffrey Rosen, *The End of Forgetting*, N.Y. TIMES, July 25, 2010, § MM (Magazine), at 30.

259. William McGeveran was quoted as making this critique in a recent New York Times article. Natasha Singer, *Technology Outpaces Privacy (Yet Again)*, N.Y. TIMES, Dec. 11, 2010, at BU3.

260. See *supra* text accompanying notes 229–234 for a description of sampling frames and how they can be used to strengthen the anonymization of data.

261. See *supra* text accompanying notes 226–228. The toughest choices will involve information that is frequently the subject of self-revelation on the Internet (e.g., preferences or movie ratings). *Id.* Also, replacing indirect identifiers with random codes does not automatically convert an indirect identifier into a non-identifier. *See supra* note 73.

(3) *Extremity-redacting* — Data producers can redact the highest or lowest value of sensitive continuous variables (e.g., income or test scores) within each subgroup if they are concerned that an adversary would be able to draw conclusions about the maximum (or minimum) value for a whole subgroup. To understand the risk this approach averts, suppose a school wishes to release a dataset containing the race, gender, and grade point average ("GPA") of its students. Suppose also that all white females at the school earned GPAs lower than 3.0. An adversary could use the database to learn that a particular white female (indeed, any white female) had a GPA below 3.0. Thus, even though the adversary cannot re-identify a particular line of data, he has learned something new and sensitive about each individual white female. If the school had redacted the highest GPA within each race-gender subgroup and replaced it with a random alphanumeric symbol, the adversary no longer knows the upper bound in the white females' (or any other group's) GPAs.[262]

(4) *Monitoring Future Overlapping Data Releases* — Finally, a data producer must ensure that it will not disclose two datasets covering the same population that can be linked through non-identifiers. Building on the race, gender, and high school GPA database example in the last paragraph, suppose the same school released a second dataset providing high school GPA and ZIP code. On its own, the second dataset seems perfectly innocuous. But any observation with a unique GPA (most likely at the bottom or top of the GPA distribution) could be linked to the first database. By doing so, an adversary can learn the race, gender, ZIP code, and GPA for those observations. This greatly increases the chance of re-identification.[263]

The theoretical concepts required to create a low-risk public dataset are not difficult when they are explained clearly and deliberately. But to this point, the judiciary has had great difficulty reasoning through and applying anonymization concepts in a principled, replicable way. The case law often contradicts itself and establishes ad hoc rules that are under- or over-protective. Even when a case reaches the

---

262. Top-coding is frequently used on income data, for a slightly different purpose than I discuss here. Income is a variable that can be used as an indirect identifier when the value is extremely high. While most people are not identifiable by their income, the very richest members of a community might be. Top-coding income to prevent this re-identification risk preserves k-anonymity and is a form of subgroup cell size control. Thus, income top-coding recodes more than just the highest income. The *Checklist on Disclosure Potential of Proposed Data Releases*, prepared by the Federal Committee on Statistical Methodology, suggests top-coding the upper limit of income distributions. Working Paper No. 22, *supra* note 109, at 103. Additional measures may be taken if a subgroup is too homogeneous with respect to a sensitive attribute.

263. Databases rarely cover the same populations since data producers have noted the high risk of overlapping disclosures on the same sample population. *See* Working Paper No. 22, *supra* note 109, at 82.

correct outcome, the analysis is often incomplete or inarticulate in its reasoning.

Consider the opinion from *Fish v. Dallas Independent School District*, discussed at length in Part II. Though the opinion applies the PII framework and properly finds that the requested dataset would run afoul of FERPA, the opinion uses flawed reasoning. The court focuses on the fact that one expert witness was able to use publicly available information to trace the identities of 550 of the Dallas students at one of the elementary schools in "less than one minute."[264] Processing speeds bear no relation to the relative ease or difficulty of re-identifying a person in a dataset. It is the discretionary decision making that comes before the computation — the skill and special information (if any) known by the human writing the attack code — that determines whether a dataset is at risk of re-identification or not.

Other cases do worse by mechanically applying statistical rules in inappropriate circumstances.[265] Consider the case of *Long v. IRS*.[266] At the trial level, the plaintiff succeeded in enforcing an old consent decree that required the Internal Revenue Service ("IRS") to release statistical reports to the plaintiff and to the public at large.[267] The issue in the case was whether one particular table that reported the number of hours spent auditing tax returns and the additional tax dollars collected through those audits violated the privacy rights of the audited taxpayers.[268] The statistics were broken down according to type of tax return, industry, and the income level of the audited taxpayer.[269]

The IRS argued that the table violates taxpayer privacy because the table contained "cells of one" — cells that described a single audited taxpayer.[270] In other words, the IRS argued that the table would violate the principle of minimum subgroup size. The plaintiff countered by arguing that "a reader would not be able to identify the taxpayer unless he already knew that the taxpayer had been audited in the relevant time period."[271] That is to say, the plaintiff was arguing that the table had an unknown sampling frame so that, in the absence of special information, an adversary would not know who was audited,

---

264. Fish v. Dallas Indep. Sch. Dist., 170 S.W.3d 226, 231 (Tex. App. 2005).

265. The California Supreme Court recently came to the preposterous holding that ZIP codes, alone, constitute "personal identification information." Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612, 615, 618 (Cal. 2011). The defendant had used ZIP codes in conjunction with names in order to find the addresses of customers (and then used the data for marketing purposes). *Id.* at 615. The court could have solved this consumer privacy problem by ruling that ZIP codes, *when combined with names*, constituted PII. Instead they expanded the definition of PII to absurd proportions by finding that ZIP codes alone are PII. *Id.* at 620.

266. 395 F.App'x 472 (9th Cir. 2010).

267. Long v. IRS, No. C74-724P, 2006 WL 1041818, at *6 (W.D. Wash. Apr. 3, 2006).

268. *Id.* at *3.

269. *Id.*

270. *Id.*

271. *Id.*

and thus could not know who was being described in the table. So, even if the table reported the audit outcome for just one medical doctor, an adversary would not be able to determine which of the country's many medical doctors had been audited. The IRS responded that publicly available information, such as press releases or public Securities and Exchange Commission ("SEC") filings, could be used to determine the identities of some taxpayers in the sampling frame.[272] The trial court found that the IRS's position was "speculative at best," and noted that the government had provided no evidence to support its claim that a cell of one could be combined with public information to identify a taxpayer.[273] The district court properly focused on whether the sampling frame was sufficiently unknown and made a factual determination in the plaintiff's favor.

The Ninth Circuit reversed and left an illogical and unsound precedent in its wake. First, the appellate court mischaracterized the district court's opinion, claiming that the lower court had considered the table to be effectively anonymized once direct identifiers had been removed.[274] Having constructed this straw man, the appellate court went too far in knocking it down: "[W]e hold that tax data that starts out as confidential return information associated with a particular taxpayer maintains that status when it appears unaltered in a tabulation with only the identifying information removed."[275] The court determined that cells of two, on the other hand, do not implicate privacy concerns.[276] The Ninth Circuit has created a test (no cells of one) that will be over- and under-inclusive in targeting re-identification risk. The court applies a threshold that is too low for minimum subgroup size (two, as compared to the standard thresholds over three) without any regard for the protective power of the unknown sampling frame.

The unknown sampling frame principle is at the root of much confusion in U.S. privacy policy.[277] Government agencies assigned with the task of providing guidance to data producers have bungled their efforts in this regard. For example, in discussing cell size limitations, Working Paper No. 22 — a guideline for federal data disclosures — provides the following as an illustration of an aggregated statistical table with disclosure risk:

---

272. *Id.*

273. *Id.* at *4.

274. Long v. IRS, 395 F.App'x 472, 475 (9th Cir. 2010).

275. *Id.*

276. *Id.* at 475–76.

277. Some courts have gotten it right. *See, e.g.*, Conn. Dep't of Admin. Servs. v. Freedom of Info. Comm'n, No. CV 95550049, 1996 WL 88490 (Conn. Super. Ct. Feb. 9, 1996) (finding that a table showing the percentage of job applicants for a librarian position that identified themselves as having a physical handicap was not privacy-violating because the pool of applicants could not be identified).

Table 1: Number of Delinquent Children by County and Education Level of Household Head[278]

Education Level of Household Head					
County	Low	Medium	High	Very High	Total
Alpha	15	**1***	**3***	**1***	20
Beta	20	10	10	15	55
Gamma	**3***	10	10	**2***	25
Delta	12	14	7	**2***	35
Total	50	35	30	20	135

The highlighted cells are supposedly problematic, because they contain fewer than five respondents.[279] But the Federal Committee on Statistical Methodology ("FCSM") mindlessly applied the minimum subgroup count rule without grounding it in a principled theory. It is true that only one of the delinquent children lives in Alpha County with a medium-educated head of household. But that delinquent child is not in danger of being re-identified. An adversary has no way of knowing who is in this sample of delinquent children unless the adversary already knows the child is delinquent. Knowing that some child lives in Alpha County with a medium-educated head of household also tells the adversary nothing about whether that child is delinquent because he cannot determine whether that child is in the sample. If the adversary did know that some particular target is in the sample, he would already know the most potentially harmful information about the target: that the target is a delinquent child.[280] When the conditions of an unknown sampling frame are met, the cell sizes have no relation to the hypothetical abuses that could flow from tabular data.[281]

In another brief, FCSM suggests that the problem with small cells in a simple frequency table like this is that anyone privy to the infor-

278. Working Paper No. 22, *supra* note 109, at 16.

279. *Id.*

280. The table could pose problems if there are very few highly educated parents in a given county. Suppose, for example, that Alpha County had only one head of household with very high education. Then members of the community might be able to discern that the head of household in question has a delinquent child. The definition of "unknown sampling frame" provided earlier in this section guards against these scenarios.

281. In the discussion of *Southern Illinoisan* in Part III, I discuss how an aggregated table can be used to slightly increase the chance of re-identification when used by a sophisticated adversary (of dubitable existence), but small cell sizes are no more vulnerable than large ones for these tactics.

mation about one of the data subjects is more likely to be able to identify the other people described in the same, small cell.[282] This suggestion may sound reasonable, but it does not logically follow. Consider the parents of a delinquent child, who know without ambiguity where their child falls in the frequency table. Even if their child was one of the two delinquent children from Gamma County with a head of household with very high education, that parent could not learn anything about the identity of the other delinquent child unless they already knew the county and education level associated with that delinquent child (in which case, they would know all there is to know).

My criticism of this exemplar table is not meant to imply that tables of aggregated information cannot breach privacy. They can and they have. The following table reports pass rates for the No Child Left Behind Exit Exam for a single high school in California. This table shows how the results were reported in public documents by the California Department of Education.

Table 2: California High School Exit Exam (CAHSEE) Results for Mathematics and English Language Arts (ELA) by Gender and Ethnic Designation, (Combined 2008) for (Grade 11)

[Name of School Redacted][283]

	MATH		**ELA**	
	Took	**Passed**	**Took**	**Passed**
All Students	**27**	**3**	**23**	**3**
Female	4	n/a	3	n/a
Male	23	3	20	2
Hispanic or Latino	20	3	18	3
White	7	n/a	5	n/a

282. CONFIDENTIALITY AND DATA ACCESS COMM. & FED. COMM. ON STATISTICAL METHODOLOGY, CONFIDENTIALITY AND DATA ACCESS ISSUES AMONG FEDERAL AGENCIES 4 (2001), *available at* http://fcsm.gov/committees/cdac/brochur10.pdf ("For example, a two-dimensional frequency count table may have rows corresponding to employment sectors (industry, academia, nonprofit, government, military) and columns corresponding to income categories (in increments of $10,000). . . . Using this example, such a tabulation could result in a disclosure of confidential information if . . . only 2 cases of any sector fell into the same income category (permitting the conclusion on the part of anyone privy to the information about one of the cases, to know the income of the other).").

283. Muralidhar & Sarathy, *supra* note 168, at 9 (table reformatted by author).

This table violates privacy by revealing the math test results with certainty for female and white students, despite the school district's effort to redact results for cells smaller than ten by replacing the number with "n/a."[284]

Blame for deficient anonymization does not reside with the data-producing agencies alone. Regulators charged with the task of setting out standards for data sharing seem to go out of their way to avoid clarity.[285] Working Paper No. 22 runs through a menu of options for data producers, including random sampling, top-coding, adding random noise, and blurring or clustering the indirect identifier variables.[286] But the paper does not provide a uniform guideline, admitting that "there are no accepted measures of disclosure risk for a microdata file, so there is no 'standard' that can be applied to assure that protection is adequate."[287]

This guidance is stunningly inadequate for a small firm or public agency charged with the task of producing a public-use dataset. It is understandable that statistical agencies would not want to commit themselves to a list of indirect identifiers or to a specific fixed set of protocols. Identifying which variables are indirect identifiers requires some working knowledge of the dataset and the publicly available resources that can be matched to the dataset. But the privacy regulators fail even to elucidate workable principles.[288] The regulatory body that administers HIPAA, for example, has failed to provide clear guidance on "specific conditions that must be met in order for privacy

---

284. *Id.*

285. This is how the FPCO responded to requests for better guidance on the application of education privacy law to de-identified data:

> In response to requests for guidance on what specific steps and methods should be used to de-identify information . . . it is not possible to prescribe or identify a single method to minimize the risk of disclosing personally identifiable information in redacted records or statistical information that will apply in every circumstance . . . . This is because determining whether a particular set of methods for de-identifying data and limiting disclosure risk is adequate cannot be made without examining the underlying data sets, other data that have been released, publicly available directories, and other data that are linked or linkable to the information in question.

Family Educational Rights and Privacy, 73 Fed. Reg. 74,806, 74,835 (Dec. 9, 2008). The FPCO is abandoning its responsibility to provide guidance on anonymization practices because it cannot provide a fool-proof step-by-step instruction manual applicable to every scenario.

286. Working Paper No. 22, *supra* note 109, at 24–33.

287. *Id.* at 24.

288. The Checklist on Disclosure Potential of Proposed Data Releases succeeds in providing some guidance on the sort of issues that must be considered when preparing a public-use microdata file. *See* INTERAGENCY CONFIDENTIALITY AND DATA ACCESS GROUP, FED. COMM. ON STATISTICAL METHODOLOGY, CHECKLIST ON DISCLOSURE POTENTIAL OF PROPOSED DATA RELEASES 6–17 (1999), *available at* http://fcsm.gov/committees/cdac/checklist_799.doc. But the guidance goes over the heads of the average government administrator, unfamiliar with "sampling frame[s]," "matching," and "nesting variables." *Id.* Like the other resources, the Checklist increases concern without providing clear principles.

risks to be minim[ized]," leaving the details to be sorted out by individual privacy boards and Institutional Review Boards.[289]

The result is complete chaos. Simply, there are no standard privacy practices. Richard Sander, a law professor at University of California, Los Angeles, recently requested anonymized admissions data from 100 public colleges and 70 public law schools.[290] The requests were submitted pursuant to an effort to conduct a systematic examination of admissions practices, but the data collection process serves as its own meta-experiment on public records compliance. Since Sander sent identical requests to every school, their responses provide a unique opportunity to observe the variance in interpretations of education privacy laws. The meta-experiment produced two important insights. First, the schools had widely divergent interpretations of their obligations under FERPA. Some of the schools complied with the FOIA requests right away and without redactions, but the majority provided data only after protracted negotiations lasting as long as two years. One fifth of the schools refused even dramatically scaled-back requests that presented no appreciable risk of re-identification. Second, the diversity among state FOIA statutes and privacy laws had little bearing on a school's likelihood to provide data. Noncompliant schools shared their state borders with compliant ones. Some of the refusing schools sent letters denying the request on the basis of privacy exemptions to the state's public records laws. Other schools became nonresponsive in the course of negotiations.[291] And a few schools effectively denied the request by sending data that redacted race information or by charging excessive fees.[292]

The void in standard practices naturally heightens the fears of members of the public, who view inconsistency as evidence that their

---

289. Barbara J. Evans, *Congress' New Infrastructural Model of Medical Privacy*, 84 NOTRE DAME L. REV. 585, 626 (2009).

290. Professor Sander's raw data and other study materials are on file with the author and are being used with permission from Professor Sander.

291. These schools received several inquiries in a variety of formats, including, at the very least, two mailed letters, two e-mails, and two phone calls. The project's logs for schools that were unresponsive read like parodies of bureaucratic inefficiency. Here is an example (names and contact information redacted):

> [10/17] VW said she never got [the request], and to speak to ES. [Phone number]. Spoke to ES, told her we would resend request. ASW 6/5: Letter mailed and emailed to ES. ASW 6/13: Recd email from ES acknowledging request and advising that it would be more than $150; they will advise us of the cost soon. TP 8/15/8 spoke with ES who said she does not remember our request but will check on it and get back to us. TP send a follow-up e-mail to [email address] // 11/19/08 ES assistant said she is out of the office for the week. Lft msg on voice mail.//12/09/08 TP got a hold of ES who connected me to vice Chancelor JP. JP asked that I e-mail him the requests. I did on same day.//1/9/9 TP left phone message for JP.

292. The University of Maryland Law School invoiced Professor Sander $3,700 for the data — an amount thirty-seven times the average cost estimates.

confidentiality may not be sufficiently protected.[293] The discrediting of anonymization and the growing perception that current privacy protocols are a fragile facade have already taken a toll on the data commons. Some public-use datasets require researchers to sign notarized affidavits and cut through a good deal of red tape before and during their use of the data.[294] And some agencies have pulled public datasets into on-site research enclaves.[295] These trends increase the costs of doing research. Some policymakers are interfering with agencies' ability to release research data at all: the Department of Transportation and Related Agencies Appropriations Act was the first federal law prohibiting access to records in the absence of individual opt-in consent, even though the records were previously open to the public and had not been the subject of any known abuses.[296] Conditioning the collection of certain categories of information on the consent of the consumer is fatal to the collection of any reasonably useful data.[297]

The stakes for data privacy have reached a new high-water mark, but the consequences are not what they seem. We are at great risk not of privacy threats, but of information obstruction.

VI. CONCLUSION: THE TRAGEDY OF THE DATA COMMONS

The contours of the right to privacy are in the grips of an existential crisis. Social networking, history-sniffing cookies, and costless

---

293. CHARLES J. SYKES, THE END OF PRIVACY 135 (1999) (noting that, in the context of medical privacy, "[i]n an age where . . . medical datawebs cover the country from coast to coast, only uniform standards have any reasonable prospect of assuring patient confidentiality"); Andrew B. Serwin, *Privacy 3.0 — The Principle of Proportionality*, 42 U. MICH. J.L. REFORM 869, 875 (2009) (finding that inconsistent legal standards cannot meet society's need for privacy).

294. The instruction manual for applying to use a dataset held by the National Center for Education Statistics is fifty-six pages long. *See* INST. OF EDUC. SCIS., U.S. DEP'T OF EDUC., RESTRICTED-USE DATA PROCEDURES MANUAL (2011), *available at* http://nces.ed.gov/pubs96/96860rev.pdf.

295. The National Center for Health Statistics ("NCHS") changed their data access policies in 2005 and pulled some previously public data files into a research enclave that requires pre-approval and the payment of a fee. *See NCHS Data Release and Access Policy for Micro-data and Compressed Vital Statistics Files*, CENTERS FOR DISEASE CONTROL AND PREVENTION, http://www.cdc.gov/nchs/nvss/dvs_data_release.htm (last updated Apr. 26, 2011). For a description of the process to apply for access to the research enclave, see *NCHS Research Data Center*, CENTERS FOR DISEASE CONTROL AND PREVENTION, http://www.cdc.gov/rdc (last updated Nov. 3, 2009).

296. Department of Transportation and Related Agencies Appropriations Act, Pub. L. No. 106-69, § 350, 113 Stat. 986, 1025–26 (1999); Cate, *supra* note 9, at 12.

297. Cate, *supra* note 9, at 15. Opt-in requirements produce insurmountable selection bias problems because the people who opt into the study (or those that do not) often share characteristics. Researchers cannot assume that the subjects who have chosen to opt in are typical or representative of the general population. Bas Jacobs, Joop Hartog & Wim Vijverberg, *Self-Selection Bias in Estimated Wage Premiums for Earnings Risk*, 37 EMPIRICAL ECON. 271, 272 (2009).

digital archiving have forced us to grapple with new and difficult problems. There are many worthy targets for the worries of privacy scholars. Research data is not one of them.

Parts II–IV of this Article analyzed the risk and the utility of public research data. With high benefit and low risk, the inescapable conclusion is that current privacy risks have little to do with anonymized research data, and the sharing of such data should be aided by the law rather than discouraged by it. But the proposals in Part V will no doubt be controversial. Now that researchers, legal scholars, and major policymakers have converged on an alarmist interpretation of the current state of data sharing, cool-headed balancing between risks and benefits is extraordinarily difficult. Our collective focus has been set on detriment alone.

Paul Ohm refers to the "inchoate harm[s]" of datasets that are released without airtight protections against re-identification.[298] Conceived of this way, the right to not be re-identified is one that need not bend to *any* considerations for the public interest in reliable research data. Ohm's approach to privacy policy is the same as my own — he advocates a balancing of the interests in privacy against the interests in data release.[299] Ohm and I arrive at very different policy proposals because we have divergent estimations of re-identification risks and the value of public data releases. However, other scholars have encouraged privacy law to drift into a property-based enforcement regime.[300] Proponents of property entitlement would say, "It is *my* data, and I want it out of the data commons." To conclude this Article, I highlight the features that make a property regime in anonymized data unworkable and unwise. Because risk is borne by individuals while utility is spread across the entire community, circumstances are ripe for a tragedy of the commons. The tort liability model for enforcement of privacy rights is much more sensible since tort liability rules are tailored to the risks and costs at a higher level of generality — the societal level.

A. Problems with the Property Model

There is no Pareto-optimal way to share data. This, unfortunately, is irrefutable. Though we are collectively better off with public re-

298. Ohm, *supra* note 4, at 1749. The term "inchoate harm" is inappropriate in the context of research data. It evokes images of a loaded gun — something nefarious and unnecessarily dangerous. Privacy harms can be described as "inchoate" when a sensitive piece of information has been exposed to public view, and it is unclear whether or when it will be harmfully linked to a data subject. *See id.* at 1749–50. This is an excellent approach for data spills (the accidental release of identifiable data). But in anonymized form, research data is no different from the data banks sitting on a server or even a personal computer. While it is susceptible to an intervening wrong, its existence is not, in itself, wrongful.

299. Ohm, *supra* note 4, at 1736.

300. *See supra* note 6.

search data, sharing data imposes risk on the data subjects. This risk can be greatly reduced by taking certain precautions, but it can never reach zero. Who, then, is to decide how much risk is too much?

Many people want (and probably believe they have) a property interest in information that describes them.[301] The practical significance of enforcing privacy rights through the property model is that the data subject retains the right to hold out. Thus, recent class action lawsuits for releasing research data demanded injunctions against sharing data in the future and brought claims for trespass to chattels.[302] Additionally, Lawrence Lessig, Jerry Kang, and Paul Schwartz have argued that Americans should have control over their information that is at least as strong as a property regime would permit and preferably stronger.[303]

In the case of research data, the property model is the wrong choice, not only for efficiency reasons, but also because it fails to meet the distributional goals required for justice.[304] Americans are naturally distrustful about data collection. Significant segments of the population continue to evade U.S. Census reporting, despite both the legal mandate to do so[305] and the Bureau's clean confidentiality record during the last six decades.[306] If data subjects refuse to consent to even small amounts of risk, which a rational actor model would predict they would do, then the data commons will dwindle as property is claimed.[307]

---

301. For example, in the complaint of a lawsuit against Apple for the disclosure of data (which Apple claims was anonymized), the data was described as "confidential information and personal property that [the data subjects] do not expect to be available to an unaffiliated company." Complaint at 5, Lalo v. Apple Inc., 2010 WL 5393496 (N.D. Cal. Dec. 23, 2010) (No. 5:10-cv-05878-PSG) [hereinafter Apple Complaint].

302. *See, e.g.*, In re Pharmatrak, Inc., 329 F.3d 9, 16 (1st Cir. 2003); Apple Complaint, *supra* note 301.

303. *See supra* note 6. Paul Schwartz challenges a simple property model for information privacy by noting that consumers will foreseeably sell their alienable information for too little compensation. Schwartz, *supra* note 6, at 2091. Schwartz embraces many of the aspects of a property model, but also proposes that government regulation should provide a right of exit (or claw-back) and a realm of inalienability. *Id.* at 2094–116.

304. The sound choice between liability and property rules will look to both efficiency and distributional goals. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1110 (1972) (explaining how liability rules facilitate the combination of efficiency and distributive results which would be difficult to achieve under property rules).

305. Eleanor Singer, Nancy A. Mathiowetz & Mick P. Couper, *The Impact of Privacy and Confidentiality Concerns on Survey Participation: The Case of the 1990 U.S. Census*, 57 PUB. OPINION Q. 465, 479 (1993).

306. While the U.S. Census Bureau has had no recent (known) confidentiality breaches, the Bureau did transfer confidential records to the U.S. Department of Justice during World War II to facilitate identifying and rounding up Japanese-Americans and placing them into internment camps. *See* JR Minkel, *Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II*, SCI. AM. (Mar. 30, 2007), http://www.scientificamerican.com/article.cfm?id=confirmed-the-us-census-b.

307. *See* Hardin, *supra* note 8, at 1244. Each data subject will view their decision to take their own data out of the commons as the optimal choice: the data commons is rich enough

This problem is analogous to the modern vaccine controversy. Children under the age of vaccination are often at the greatest risk of death from virulent diseases like whooping cough.[308] The best protection is for everyone else (of eligible age) to get the vaccine, even though the vaccine itself poses dubious but popularly accepted risks.[309] Parents who choose not to vaccinate their children expect to have it both ways: since everyone else is vaccinated, their child is unlikely to be exposed to the virus or disease. But they also avoid the small chance that their child could have an adverse reaction to the vaccination. The trouble is, once enough parents opt out of the vaccination pool, the communal protection falls apart. Thus, we are now witnessing a resurgence in infant mortality from whooping cough because the virus is spreading among adults and older children, who historically had been vaccinated but no longer are.[310]

Like the communal vaccination shield, the data commons is especially vulnerable to opt-outs. As people opt out, the value of the overall data diminishes precipitously rather than linearly: even a small number of holdouts will produce selection bias effects that compromise the utility of the remaining data. Khaled El Emam, Elizabeth Jonker, and Anita Fineberg have recently compiled and analyzed the evidence of selection bias caused by consent requirements to perform research on observation health data — data that was already collected in the course of treatment, such that research requires no additional interaction with the patients.[311] Consent is denied more frequently by patients who are younger, African American, unmarried, less educated, of lower socio-economic status, or — importantly — healthy.[312] These patterns are very difficult to control for, and they cause distortions in health research.[313] Put bluntly, property rights that follow the information into the data commons (and allow the data to be clawed

---

to allow for research, but their own data is not exposed to risk of re-identification. If many people arrived at this same choice in the course of their own independent evaluations, there would be no commons left. I discuss the differences between the data commons and the traditional tragedy of the commons in Part I. *See supra* note 8.

308. *See generally Pertussis (Whooping Cough)*, CENTERS FOR DISEASE CONTROL & PREVENTION, http://www.cdc.gov/pertussis/index.html (last updated Aug. 22, 2011).

309. *See* Chris Mooney, *Why Does the Vaccine/Autism Controversy Live On?*, DISCOVER MAG., June 2009, at 58, 58–59.

310. Ijeoma Ejigiri, *The Resurgence of Pertussis: Is Lack of Adult Vaccination to Blame?*, CLINICAL CORRELATIONS (Feb. 23, 2011), http://www.clinicalcorrelations.org/?p=3951.

311. Khaled El Emam et al., The Case for De-identifying Personal Health Information 21–29 (Jan. 18, 2011) (unpublished manuscript), *available at* http://ssrn.com/abstract=1744038.

312. *Id.* at 27.

313. *Id.* at 25–28.

back out) would allow holdouts to wreak disproportional havoc on research.[314]

The impulse to enforce research data privacy rights through property rules should be jettisoned and a tort approach restored.[315] On this issue, Paul Ohm and I agree that the public interest is best served by asking whether the utility of a public dataset significantly outweighs the risk of harm.[316] This would mark a return to the rational balancing anticipated by Samuel Warren and Louis Brandeis, who recognized that privacy rights should not interfere with information flow when that information is socially valuable.[317] This balancing of risks and benefits will also realign the policy discourse with the anonymization practices that are already widely in use and embraced by privacy experts in the statistics and social science fields. Anonymization was never believed to be a "privacy-providing panacea."[318] As Douglas Sylvester and Sharon Lohr correctly assert, "[t]he law, in fact, does not require that there be absolutely no risk that an individual could be identified from released data."[319] Rather, the law was assumed to reflect a conservative position in the risk-utility analysis — and it still does.

Radical as they may sound, this Article's proposals are formally reconcilable with the privacy scholarship that demands inalienable rights in the control of information. De-identified (anonymized) data need not be considered as relating to the underlying data subject at all — unless and until their data has been re-identified. The theoretical foundations for establishing a distinct regime for anonymized data are already in existence. Jerry Kang has noted that privacy is in some tension with intellectual property since there is no available copyright ownership interest in facts.[320] Once data has been unlinked from an identifiable person, perhaps it is best understood as a fact in the public domain. Better still, Ted Janger and Paul Schwartz have proposed a

---

314. If a property rule is crafted to avoid over-protection then it will likely end up in a form that is under-protective. Suppose we were to determine that the data subject had alienated his right to the information as soon as he gave it to the data producer (say, a retailer or his doctor), then a property regime would constrain the state from interfering with the data producer's use, no matter how badly the original data subject was under-compensated. This is not sound policy in the majority of contexts in which data is collected — where the information is given for a purpose without concrete attention to the additional uses (in identifiable form or not) to which the data will be put.

315. Fred Cate has argued that democratic values would benefit from a shift away from property rights, though he sees value, often overlooked by the legal academy, in allowing private entities to use data for secondary uses. *See* Cate, *supra* note 9, at 12.

316. Ohm advises regulators to compare the risks of unfettered information flow to its likely costs in privacy. Ohm, *supra* note 4, at 1768.

317. Warren & Brandeis, *supra* note 43, at 214.

318. Ohm, *supra* note 4, at 1716.

319. Douglas J. Sylvester & Sharon Lohr, *Counting on Confidentiality: Legal and Statistical Approaches to Federal Privacy Law after the USA Patriot Act*, 2005 WIS. L. REV. 1033, 1113 (2005).

320. Kang & Buchner, *supra* note 6, at 233.

move to "constitutive privacy" rights, where access to information and limits on it should be modeled with an eye toward the nature of our society and the way we like to live.[321] Here the "democratic community"[322] is much better served by relinquishing an individual's control over anonymized research data.

Detaching privacy rights from anonymized data presents the best option available because it prevents what Anita Allen calls the maldistribution of privacy.[323] Consider the following scenario: a school district wishes to test a theory that implicit biases cause its teachers to depress grades of minority students when students are evaluated on subjective criteria. To test the hypothesis, the school district uses the objective scores received by its students on validated exams as controls to see if minority students receive significantly lower grades when grading is left to the teacher's subjective judgment. A small set of parents, after catching wind of the study, object to the use of their (Caucasian) children's data because the secondary use of their children's information does not suit their interests. Should we consider the data, in anonymized form, to be *their* data? Individuals' control over research data would result in a maldistribution of knowledge.

B. The Data Subject as the Honorable Public Servant

The data commons is the tax we pay to our public information reserves. Danielle Citron and Paul Schwartz have persuasively argued that privacy is a critical ingredient to a healthy social discourse.[324] In many respects this is true, but if taken to the extreme, data privacy can also make discourse anemic and shallow by removing from it relevant and readily attainable facts.

In time, technological solutions are likely to pare down the existing tension between data utility and disclosure risk.[325] Statistical software that allows the dataset to remain on a secure server while researchers submit statistical queries has been developed, and many

---

321. Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1250–51 (2002).

322. *Id.* at 1251.

323. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 725 (1999) ("Neither privacy nor private choice, however, is an absolute, unqualified good. There can be too much privacy, and it can be maldistributed.").

324. Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822, 841–43 (2010); Schwartz, *supra* note 251, at 593 (1995) ("The boundless collection, processing, and dissemination of personal data can have a deleterious effect on the ability of individuals to join in social discourse.").

325. John M. Abowd & Julia Lane, *New Approaches to Confidentiality Protection: Synthetic Data, Remote Access and Research Data Centers* 3050 PRIVACY IN STATISTICAL DATABASES: LECTURE NOTES IN COMPUTER SCIENCE 282, 283 (2004), *available at* http://www.springerlink.com/content/27nud7qx09qurg3p/fulltext.pdf.

data producers are slowly beginning to implement it.[326] In the meantime, anonymization continues to be an excellent compromise. Rather than sounding alarms and feeding into preexisting paranoia, the voices of reason from the legal academy should invoke a civic duty to participate in the public data commons and to proudly contribute to the digital fields that describe none of us and all of us at the same time.

326. For example, the U.S. Census Bureau's American FactFinder service allows users to submit queries for the creation of customized tables. *American FactFinder*, U.S. CENSUS BUREAU, http://factfinder.census.gov/servlet/DatasetMainPageServlet (last visited Dec. 21, 2011).