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.