The Law and Economics of Privacy

Daniel J. Gilman and Liad Wagman*

Abstract

I. Introduction

As of August 2023, there is no general data protection law in the United States. More specifically, there is no overarching federal privacy statute. There are, however, numerous federal and state laws pertaining to privacy; and there are at least several federal enforcement agencies that have some jurisdiction over data privacy. Still, many might agree with the assertion by the Federal Trade Commission (FTC) that, "[f]or more than two decades, the Commission has been the nation's privacy agency."[1] There is at least a sense in which that may be true. The FTC does not enforce all federal privacy laws and it has not brought more privacy-related cases than any other federal enforcer.[2] Nonetheless, the Commission has brought hundreds of cases to protect the privacy and security of consumer data,[3] and the FTC's multi-sector purview is the widest ranging of the relevant

* Daniel J. Gilman is Senior Scholar, Competition Policy, at the International Center for Law & Economics; from 2006-2023, he was an Attorney Advisor in the FTC's Office of Policy Planning. Liad Wagman is Professor of Economics and the John and Mae Calamos Dean Endowed Chair, Stuart School of Business, Illinois Institute of Technology, and Academic Affiliate at the International Center for Law & Economics; from 2020-2022, he was Senior Economic & Technology Advisor in the FTC's Office of Policy Planning. We thank Bilal Sayyed for his comments on an early draft of this material; any faults that remain are the authors' alone.

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FED. REG. 51273 (Aug. 22, 2022) (to be codified at 16 C.F.R. Ch. 1) [hereinafter "ANPR" or "Commercial Surveillance ANPR"]. *But cf.* Mike Swift, *The Long Read: SEC Becomes Prominent US Cybersecurity Regulator with New Breach Reporting Rules*, mlex Data Privacy and Security News (Jul. 26, 2023), https://content.mlex.com/#/content/1488676/comment-sec-becomes-prominent-us-cybersecurity-regulator-with-new-breach-reporting-rules?referrer=search_linkclick (quoting Chris Hoofnagle, "Five years ago, the Federal Trade Commission was America's most consequential cyber regulator, but now . . . [the SEC] has emerged as the nation's most important leader in the field.")

[2] *See* notes 84-85 and accompanying text, *infra*, regarding the enforcement of the HIPAA privacy and data security rules.

[3] *See, e.g.*, Fed. Trade Comm'n, Privacy & Data Security Update: https://www.ftc.gov/reports/privacy-data-security-update-2019 (noting, through calendar year 2019, more than 130 spam and spyware cases and 80 general privacy lawsuits, including a $5 billion settlement with Facebook, id. at 2; more than 75 data security cases, including a $375 million settlement with Equifax, id. at 5; more than 100 Fair Credit Reporting Act cases, id. at 7; close to 30 cases under the Children's Online Privacy Protection Act (COPPA) since 2000, id. at 8; about 35 cases under the Gramm-Leach-Bliley Act on financial institution privacy notices, id. at 7; and almost 150 cases enforcing do-not-call provisions, id. at 10.

federal authorities. That has led some privacy scholars to suggest that, e.g., "FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States."[4]

The economic underpinnings of the FTC's approach to consumer privacy[5] are of interest for several reasons. Chief among them is the scope of the Commission's authority in privacy. Subject to certain exclusions, the FTC's privacy authority – under Section 5 of the FTC Act and under several narrower statutes – ranges across most of the economy.[6] As a result, the FTC is the primary federal inter-sectoral enforcer of privacy and data security laws in the United States. We also note that recent legislative proposals have considered extending the FTC's privacy authority.[7] And in 2022, the FTC issued an Advance Notice of Proposed Rulemaking regarding "commercial surveillance," which contemplates a broad, if not specific, domain of potential data regulation, with privacy and data security concerns at its core.[8] Although no specific regulation was proposed therein, the range of issues raised

[4] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585-586 (2011). Given that nearly all of this "new common law of privacy" consists of agency consent orders, rather than judicial opinions, one might question the extent to which this can be regarded as "jurisprudence," but it is at least a body of settlement decisions, and it can be said to offer a sort of agency guidance that is analogous to a jurisprudence.

[5] The focus of this paper is privacy, rather than data security, but we mention both throughout, and for several reasons. First, while the terms "privacy" and "data security" tend to refer to distinct concerns, they are variously related, both as a practical matter and as legal or regulatory one. For example, data security tools or practices, such as the encryption of sensitive data, may be means of implementing a privacy policy; that is, of preventing (or impeding) unauthorized access to personal information. Second, legal and regulatory matters, and economic research, often address both privacy and data security concerns, and not always in ways easily teased apart. While we do not exclude data security concerns or research from this paper entirely, we do focus on those data security issues that seem directly pertinent to privacy policies, benefits, and harms

[6] The FTC's authority ranges across most of the economy, as Section 5 pertains to "methods . . . acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1) (2012). "In or affecting commerce" is read broadly, subject to certain express exclusions. Those exclusions enumerated under Section 5 include "banks, savings and loan institutions . . . common carriers . . . air carriers and foreign air carriers . . and [certain] persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended." *Id.* at § 45(a)(2).

[7] For example, bills proposed (but not adopted) in the 117th Congress (2021-22), included the Consumer Data Privacy and Security Act of 2021, S. 1494, which would have stipulated that its violations "shall be treated as an unfair or deceptive act or practice in violation of a rule promulgated under section 18(a)(1)(B) of the Federal Trade Commission Act (15 USC 57a(a)(1)(B)); while the Data Care Act of 2021, S-919. conferred rulemaking authority on the FTC, while stipulating that implementing regulations be adopted under the less restrictive procedures of the Administrative Procedure Act, section 553 of title 5, United States Code.

[8] Note 2, *supra*.

by the notice suggests the possibility of something akin to a U.S. General Data Protection Regulation, ranging over both privacy and data security issues.[9]

In addition, the FTC is the only U.S. government agency charged generally with enforcing both competition and consumer protection laws regarding users' data. The twin missions of the FTC are often said to be complements. At the same time, one might ask about the coherence of the FTC's enforcement programs, or about the extent to which the two missions of the agency function as complements or substitutes. Relatedly, one might ask about the extent to which research in industrial organization economics or consumer protection economics might inform both programs.

Finally, the Commission's privacy policy initiatives have been diverse, extending well beyond enforcement to include "soft law" mechanisms, such as guidance for industry,[10] consumer education,[11] policy advocacy,[12] and economic and policy research. Section 6 of the FTC Act[13] provides the FTC with a type of research and advocacy authority: it enables the Commission to conduct investigations in the service of its enforcement actions, but it also provides a more general authority to investigate and report on market developments in the public interest, and it grants the Commission the authority to make legislative recommendations based on its investigations.[14]

---

[9] For one example (among many) of comments on the potential scope and implications of regulations contemplated in the FTC's Advance Notice, see, e.g., Geoffrey A. Manne, Daniel Gilman & Kristian Stout, Comments of the International Center for Law & Economics, FTC Advance Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, Docket No. FTC-2022-0053, Commercial Surveillance ANPR, R111004 (Nov. 21, 2022), https://laweconcenter.org/wp-content/uploads/2022/11/ICLE-Commercial-Surveilance-ANPR-Comments-v4.pdf.

[10] *See, e.g.*, Fed. Trade Comm'n, Consumer Privacy, FTC Bus. Guidance, https://www.ftc.gov/business-guidance/privacy-security/consumer-privacy (last checked 2/15/23).

[11] *See, e.g.*, Fed. Trade Comm'n, How to Recognize and Avoid Phishing Scams, FTC Consumer Advice (Sept. 2022), https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

[12] For an overview of the FTC's competition advocacy program, see, e.g., James C. Cooper, et al., *Theory and Practice of Competition Advocacy at the FTC*, 72 ANTITRUST L.J. 1091 (2004-05); Daniel J. Gilman, *Advocacy*, SAGE ENCYCLOPEDIA OF POLITICAL BEHAVIOR 8 (Fathali M. Moghaddam, ed. 2017).

[13] 15 USC 46.

[14] *Id.* at § 46(a), (b), and (f) (the authority to gather information or investigate "organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce," to require the reporting of pertinent information from such entities, and to publish its findings, reports, and recommendations, both for Congress and for public use, respectively).

Economic and policy research have been express parts of the FTC's statutory mission since the agency's inception. Not incidentally, the FTC employs a staff of research economists in its Bureau of Economics ("BE"), comprising both industrial organization and consumer protection economists. And the Commission and agency staff have provided a forum for the development and dissemination of both privacy and data security research.[15] In recent years, the FTC has, among other things, hosted myriad events to promote both collaboration and the dissemination of research among privacy researchers, academics, industry representatives, consumer advocates, and government. Those events have included, *inter alia*, a public workshop on the subject of informational injury,[16] a recurring privacy-focused conference named PrivacyCon,[17] and several hearings sessions on privacy and data security issues in the FTC's Hearings on Competition and Consumer Protection in the 21st Century.[18] The latter include separate multiday sessions on the FTC's Approach to

---

[15] Those contributions include both official reports of the Commission and research by FTC personnel. *Compare*, *e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS (2012) (FTC Report) *with* Ginger Zhe Jin & Andrew Stivers, *Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics*, SSRN Working Paper (May 22, 2017), https://ssrn.com/abstract=3006172 or http://dx.doi.org/10.2139/ssrn.3006172; Dan Hanner, Ginger Zhe Jin, Marc Luppino, & Ted Rosenbaum, *Economics at the FTC: Horizontal Mergers and Data Security*, 49 REV. INDUS. ORG. 613 (2016) (section on estimating harm from data breaches with application to *Wyndham* at 627 – 630); Maureen K. Ohlhausen and Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L. J. 121 (2015); Joseph Farrell, *Can Privacy be Just Another Good?*, 10 J. ON TELECOMM. & HIGH TECH. L. 251 (2012); Daniel J. Gilman & James C. Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is Which: Striking The Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279 (2010); James C. Cooper & Joshua D. Wright, The Missing Role of Economics in FTC Privacy Policy, in CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Evan Selinger et al., eds., 2018); J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 118–20 (2008) (published after the authors, a former Chairman and a former Director of the Bureau of Consumer Protection, had left the agency).

[16] Fed. Trade Comm'n, Informational Injury Workshop (Dec. 12, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop.

[17] *See, e.g.*, Fed. Trade Comm'n, PrivacyCON 2018 (Feb. 28, 2018), https://www.ftc.gov/news-events/events-calendar/2018/02/privacycon-2018; Fed. Trade Comm'n, PrivacyCON 2020, https://www.ftc.gov/news-events/events-calendar/privacycon-2020 (announcing Jul. 2020 PrivacyCON).

[18] Fed. Trade Comm'n, Hearings on Competition and Consumer Protection in the 21st Century https://www.ftc.gov/policy/hearings-competition-consumer-protection.

Consumer Privacy;[19] Data Security;[20] Big Data, Privacy, and Competition;[21] and Algorithms, Artificial Intelligence, and Predictive Analytics.[22]

This paper builds on the presentations and submissions to these workshops, conferences, and hearings, and on related studies. We synthesize some findings from research regarding the impact of specific privacy policies on competition, innovation, and consumer welfare,[23] reviewing these works through the lens of a research-based regulator charged to protect consumer welfare with dual competition and consumer protection enforcement mandates. Not incidentally, one of the main planks of the FTC's consumer protection authorities – its "unfairness" jurisdiction under Section 5 of the FTC Act, stipulates that conduct cannot be found "unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoided by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[24] That is, privacy enforcement decisions or regulations based on the unfairness authority require an assessment of consumer welfare effects and economic tradeoffs, including an assessment of the likely impact of intervention on competition. There is also a nexus with the FTC's "deception" authority under Section 5, to the extent that unlawful representations or omissions must be material ones; that is, those "likely to affect the consumer's conduct or decision with regard to a product or service," and where "consumer injury is likely," due to the deception.[25]

---

[19] Fed. Trade Comm'n, Hearings on Competition and Consumer Protection in the 21st Century, the FTC's Approach to Consumer Privacy (Apr. 9-10, 2019), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019

[20] Fed. Trade Comm'n, Hearings on Competition and Consumer Protection in the 21st Century, Data Security (Dec. 11-12, 2018), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018.

[21] Fed. Trade Comm'n, Hearings on Competition and Consumer Protection in the 21st Century, Big Data, Privacy, and Competition (Nov. 6-8, 2018), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-6-competition-consumer-protection-21st-century.

[22] Fed. Trade Comm'n, Hearings on Competition and Consumer Protection in the 21st Century, Algorithms, Artificial Intelligence, and Predictive Analytics (Nov. 13-14, 2018), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-7-competition-consumer-protection-21st-century.

[23] For a general overview of economic issues regarding privacy, see, e.g., Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442 (2016).

[24] 15 U.S.C. § 45(n).

[25] FTC Policy Statement on Deception, Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf. Note

The consumer welfare focus of the FTC's established jurisdiction under the FTC Act – as commonly accepted, at least prior to the current administration – thus serves as an organizing principle, reaching diverse issues in both competition and consumer protection data policy. The Act's focus on consumer welfare also provides a uniform basis on which to consider the diverse tradeoffs that privacy policies entail, and one that's amenable to empirical investigation. Our discussion should, therefore, be of interest to FTC privacy, and to some extent data security, enforcement, which ranges across much of the U.S. economy, but it should be of broader interest as well. Policy makers may have concerns well beyond those of FTC enforcement policy, and they may have diverse goals in policymaking. At the same time, a consumer welfare focus should be of broader policy interest, to the extent that economic research pertaining to privacy and data security issues, a policy perspective reflecting both competition and consumer protection concerns, and an underlying concern with regulation and law enforcement in the service of – and constrained by – consumer welfare, may inform policy considerations beyond the Commission's ambit.[26]

We recognize too, that present FTC leadership has questioned the import, and legal foundations, of the consumer welfare standard that has long dominated both U.S. antitrust law and the Commission's understanding of its unfairness authority under Section 5 of the

too that Section 12 of the FTC Act, prohibits false ads for foods, drugs, devices, and cosmetics, specifically, and that Section 15 of the FTC Act defines such prohibited ads as "material" ones. 15 U.S.C. §§ 52, 55.

[26] A policy perspective reflecting both competition and consumer protection concerns may also be relevant to the Commission's own work, to the extent that privacy-pertinent matters may present both competition and consumer protection concerns. *See, e.g.*, OECD, Directorate for Fin. and Enterprise Affs. Comp. Comm., Consumer Data Rights and Competition—Note by the United States (Jun. 12, 2020), https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/oecd-consumer_data_rights_us_submission.pdf (presented to OECD by FTC Commissioner Noah Phillips); Maureen K. Ohlhausen and Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L. J. 121 (2015); Timothy J. Muris, The Interface of Competition and Consumer Protection, Fordham Corp. Law Inst. Twenty-Ninth Annual Conf. on Int. Antitrust Law & Pol'y (Oct. 31, 2002) (prepared remarks of then FTC Chairman).

FTC Act.[27] Such assertions have been controversial.[28] While that controversy is not our focus, we acknowledge that the FTC-centric lens applied in this paper hews to a consumer welfare framework that has dominated U.S. competition and consumer protection policy in data matters and others, in the agencies and the courts, across at least several decades.

Our overarching observation comports with prior academic work from an economic perspective: privacy policies entail complex tradeoffs, both across consumers and for individuals. That may be true for policy initiatives generally, although we suggest that the complexity of the domain makes this a poignant case. Privacy is a complex concept – not a simple goal or function to be optimized – and privacy policies may entail especially complex tradeoffs. The diverse interests that constitute privacy pose distinctive challenges, as well as opportunities for policymakers.

Demonstrated and potential costs and benefits are heterogenous, and may vary across industries, data domains, or types of regulatory intervention, and not just across persons. At the same time, many privacy policy initiatives – including legislation,

---

[27] *See, e.g.*, FTC, Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act, Commission File No. P221202 (Nov. 10, 2022). Regarding privacy and data security, see, e.g., F.T.C., Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, (Aug. 22, 2022) (to be codified at 16 C.F.R. Ch. 1) [hereinafter "ANPR" or "Commercial Surveillance ANPR"]; *cf.* F.T.C., Comment of Commissioner Alvaro M. Bedoya, In the Matter of Facebook, Inc., Docket No. C-4365 (May 3, 2023) (questioning, on legal grounds, the nexus between alleged violaions and Commission's proposed order modification; that is, the new proposed remedy).

[28] *See* F.T.C., Dissenting Statement of Commissioner Christine S. Wilson Regarding the "Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act," Nov. 10, 2022, https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-of-commissioner-wilson-on-policy-statement-regarding-section-5. Daniel J. Gilman & Gus Hurwitz, The FTC's UMC Policy Statement: Untethered from Consumer Welfare and the Rule of Reason, ICLE Issue Brief (Nov. 16, 2022), https://laweconcenter.org/resources/the-ftcs-umc-policy-statement-untethered-from-consumer-welfare-and-the-rule-of-reason/. For concerns about the FTC's "Commercial Surveillance" ANPR, see F.T.C., Dissenting Statement of Commissioner Noah Joshua Phillips Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking, Aug. 11, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf; F.T.C., Dissenting Statement of Commissioner Christine S. Wilson Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking, Aug. 11, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Wilson%20Dissent%20ANPRM%20FINAL%2008112022.pdf; Geoffrey A. Manne, Daniel J. Gilman, and Kristian Stout, Comments of the International Center for Law & Economics on the FTC Advance Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, Docket No. FTC-2022-0053, Commercial Surveillance ANPR, R111004 (Nov. 1, 2022), comment No. FTC-2022-0053-0976, https://www.regulations.gov/comment/FTC-2022-0053-0976.

regulation, and enforcement – seem to lack fulsome accounting for these tradeoffs, requirements for regulatory cost-benefit analysis in the U.S. and other jurisdictions notwithstanding. Specifically – but not uniquely – attention to the competitive effects of regulation (or other interventions) has been lacking.[29] While we lack a complete picture – either theoretical or empirical – of the effects of privacy policies generally, or indeed of any specific privacy regulations, there is mounting and diverse evidence of some of the costs of extant privacy regulations. These include, but are not limited to, competitive costs; and they include unanticipated and/or unintended effects. Although there has been some research into the benefits associated with specific regulations that enhance privacy, such benefits remain understudied.

a. A Conceptual Overview of a Complex Privacy Domain

Digital commerce is an integral part of the economy. Data comprise both inputs and outputs for myriad products and services; and products and services simultaneously generate and capture digital trails. Increasingly large amounts of information about (or associated with) individual human persons,[30] groups, and firms is collected, coded, stored, and analyzed.[31] These troves of data have obvious and significant economic value, as

---

[29] For example, in proposing the HIPAA Privacy Rule, the Department of Health and Human Services made no attempt to consider, much less measure, the proposed rule's likely competitive impact. At that time, HHS estimated that the cost of compliance with the proposed rule would be at least $3.8 billion over five years. At the same time, HHS acknowledged that its "ability to measure costs of the proposed regulation is limited because there is very little data currently available on the cost of privacy protection . . . [and HHS] has not been able to estimate costs for a number of requirements of the proposed regulation that we know will impose some cost to covered entities." 64 Fed. Reg. 59918, 6006-60008 (Nov. 3, 1999).

[30] For instance, the act of listening to a podcast using a streaming service (as opposed to listening to a channel on FM radio), can be captured by the streaming service, which then can determine information about the listener's preferences. This data can be combined with other information about the individual, and then used in various manners: to compile a profile of the listener; to infer their other interests and preferences; to present them with targeted advertising; or to sell their information to data aggregators or other parties. As discussed below, we recognize that concepts of "personal information" or "personally identifiable information" vary, and that the semantics of "about" are not fully settled or uniformly understood.

[31] For example, a 2014 report on data brokers by the Federal Trade Commission observes that "one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements," and that another broker "has 3000 data segments for nearly every US consumer." Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability, iv (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Data collection, analysis, and transmission have continued apace since the publication of the 2014 report, and recent estimates suggest

signaled by, for example, the substantial market valuations of some of the leading firms in the space,[32] the relative sizes of, e.g., online advertising markets,[33] and the value of online content to consumers.[34] Recent developments in artificial intelligence (A.I.), including those in "Generative A.I." and, specifically, large language models (L.L.M.s) underscore the potential of the data economy and large data sets.[35] At the same time, the scraping and

---

total data production of 64.2 zettabytes by 2020, and over 180 zettaabytes of data by 2025 (a zettabyte is a trillion gigabytes). Petroc Taylor, Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025, Statista (2022), https://www.statista.com/statistics/871513/worldwide-data-created/. ***Do we like another source better?*** Numerous writings have tried to capture key aspects of this data expansion under the rubric "big data." Although there is no uniform definition of "big data," there is widespread interest in what is sometimes referred to as "the four Vs": "Big Data consists of extensive datasets – primarily in the characteristics of volume, variety, velocity, and/or variability – that require a scalable architecture for efficient storage, manipulation, and analysis." NIST Big Data Interoperability Framework, V. 1: Definitions, NIST Big Data Public Working Group (2018), https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1r1.pdf; *see also*, FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf ("The term 'big data' refers to a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions").

[32] *See, e.g.*, Ben Winck, *The 5 Most Valuable US Tech Companies are Now Worth More Than $5 Trillion after Alphabet's Record Close*, Bus. Insider, Jan. 17, 2020, https://markets.businessinsider.com/news/stocks/most-valuable-tech-companies-total-worth-trillions-alphabet-stock-record-2020-1-1028826533; Andrea Murphy, et al., *Global 2000: The World's Largest Public Companies*, Forbes, May 13, 2020, https://www.forbes.com/global2000/#4e83583f335d (ranking based on four metrics: sales, profits, assets and market value). ***Update citation.***

[33] *See, e.g.*, How Has The U.S. Online Advertising Market Grown, And What's The Forecast Over The Next 5 Years?, Forbes, Jun. 11, 2019, https://www.forbes.com/sites/greatspeculations/2019/06/11/how-has-the-u-s-online-advertising-market-grown-and-whats-the-forecast-over-the-next-5-years/#6dbca8246607.

[34] For example, Brynjolfsson, Collis, and Eggers use a combination of different survey methodologies to show that high levels of consumer surplus are associated with free online content. Erik Brynjolfsson, Avinash Collis & Felix Eggers, *Using Massive Online Choice Experiments to Measure Changes in Well-being*, 15 PROC. NAT'L ACAD. SCI.7520 (2019) (using willingness-to-accept estimates to show that the median consumer in 2016 valued online search at $14,760 per year and valued the rest of the Internet at $10,937 per year, or, roughly $8.3 trillion in aggregate for the U.S.). *See also*, Leonard Nakamura, et al., *"Free" Internet Content: Web 1.0, Web 2.0, and the Sources of Economic Growth*, Fed. Reserve Bank of Philadelphia Working Papers, WP 18-17 (2018), https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2018/wp18-17.pdf. Nakamura, et al. (2018) (analyzing contribution of "free" content to domestic production, and estimating addition of $294 billion to U.S. GDP, based on cost of production);

[35] Although there is no canonical definition of "Generative A.I.," a recent report by the Congressional Research Service provides a useful, if brief, overview. U.S. Cong. Res. Serv., Generative Artificial Intelligence and Data Privacy: A Primer, R47569, 1-3 (May 23, 2023) https://crsreports.congress.gov/product/pdf/R/R47569. And as noted therein, the National Artificial Intelligence Initiative Act of 2020 (P.L. 116-283) defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action."

other automated means of mass data collection employed to provide inputs into Generative A.I. have raised privacy concerns,[36] and, indeed, the prospect and onset of new regulation.[37]

The products and services that depend on personal data[38] have borne benefits for both consumers and firms. At the same time, they have been associated with actual and potential harms,[39] and concerns about the collection, flow, and use of personal information have intensified.[40] While some recently voiced concerns are not new,[41] they still raise questions about the range of conduct enabled by new technologies that should be lawful (or unlawful), and, correspondingly, about the form any regulation and legal sanction should take for conduct that ought to be prohibited or otherwise limited. At the same time,

---

[36] Generative Artificial Intelligence and Data Privacy, supra note 33, at 4-5.

[37] *Id.* at 6-7. For example, in April 2023, the FTC, U.S. Dep't Justice Civil Rights Commission, Consumer Financial Protection Bureau (CFPB), and Equal Employment Opportunity Commission Released a Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems, https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/joint-statement-enforcement-efforts-against-discrimination-bias-automated-systems. Bills introduced in the current (118th) Congress include, e.g., the AI Disclosure Act of 2023, H.R. 3831, 118th Cong (2023). We note, in Europe, the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SEC (2021) 167 final (Apr. 21, 2021). And in October 2022, the White House Office of Science and Technology Policy published a Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, identifying "five principles that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence." / The White House, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (2022) [hereinafter AI Blueprint] https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf. Although the Blueprint does not itself comprise an Executive Order, it is likely to influence diverse regulatory decisions under the Biden Administration, at least.

[38] We leave aside for now the question what constitutes "personal data."

[39] The Federal Trade Commission's 2016 report on big data highlights a number of benefits to underserved populations, including increased educational attainment, access to credit through non-traditional methods, specialized health care, and better access to employment. The report also highlights possible risks that could result from biases or inaccuracies about certain groups, including more individuals mistakenly denied opportunities based on the actions of others, sensitive information being exposed, existing disparities being reinforced, increased targeting of vulnerable consumers for reasons such as fraud, increase in prices for goods and services in lower-income communities, and the weakening of consumer choice. *See generally*, FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), *supra* note 18.

[40] Recent Pew surveys find that 81% of respondents believe they have lost control over how personal information is collected and 79% are concerned about how their data is used. PEW RESEARCH CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION, 2 (2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[41] Warren and Brandeis stated that "[i]nstantaneous photographs and 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.'" Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

given the myriad benefits generated by the information economy, such concerns may also suggest complex tradeoffs associated with both private and public decisions to collect or share, or restrict the collection, sharing, and use of, personal information.[42]

More specifically, the sharing of personal information can entail both benefits and costs for individual human persons and for social welfare. People can benefit, directly and indirectly, by sharing information about themselves, or by allowing others to collect information about them. Such benefits can be tangible or intangible. They may include, *inter alia*, better quality and more efficient medical care,[43] the personalized services and discounts one receives after joining a merchant's loyalty program,[44] or the reduced search costs and increased relevance or accuracy of information retrieval one can experience when tracked more closely by a service provider, such as a search engine or a mapping service.[45] When consumers withhold (or do not permit access to) information, they may forgo those benefits; and those forgone benefits can be viewed as opportunity costs that they bear.[46]

Sharing information about oneself can also entail costs. For example, in 2019, the Department of Housing and Urban Development alleged that, because of the way Facebook (now Meta) designed its advertising platform, "ads for housing and housing-related services are shown to large audiences that are severely biased based on characteristics

---

[42] Westin (1967) used non-context specific broad privacy questions in surveys to cluster individuals into privacy segments: privacy fundamentalists, pragmatists, and unconcerned. ALAN F. WESTIN, PRIVACY AND FREEDOM, (1967). When asked directly, many people fall in the first segment, professing to care a lot about privacy and express concern over losing control of their personal information or others gaining unauthorized access to it. However, individuals' willingness to pay to preserve their data is often relatively small. *See, e.g.*, Scott J. Savage & Donald M. Waldman, Privacy Tradeoffs in Smartphone Applications, 137(c) ECON. LETTERS 171 (2015). This dichotomy in stated privacy preferences and privacy behavior has been called the "privacy paradox." *See, e.g.*, Daniel J. Solove, *The Myth of the Privacy Paradox* (February 11, 2020). 89 GEO. WASH. L. REV. (2021) (forthcoming).

[43] *See, e.g.*, Hilal Atasoy, Brad N. Greenwood & Jeffrey Scott McCullough, *The Digitization of Patient Care: A Review of the Effects of Electronic Health Records on Health Care Quality and Utilization*, 40 ANN. REV. PUB. HEALTH 487 (2019) (reviewing and synthesizing literature regarding effects of electronic health records); Jennifer King, et al., *Clinical Benefits of Electronic Health Records Use: National Findings*, 49 HEALTH SERVS. RES. 392 (2014).

[44] ***Get newer cites to marketing literature.*** Frederick F. Reichheld & W. Earl Sasser, Zero Defections: Quality Comes to Services, Harv. Bus. Rev. (Sept.-Oct. 1990).

[45] Diana I. Tamir & Jason P. Mitchell, *Disclosing Information About the Self Is Intrinsically Rewarding*, 109 PROC. NAT'L ACAD. SCI. (PNAS) 8038 (2012).

[46]

protected by the Act, such as audiences of tens of thousands of users that are nearly all men or nearly all women."[47] It was also alleged that Facebook provided tools that could facilitate discrimination by third parties.[48] Information could also be used to charge individuals prices closer to their reservation values.[49]

Both positive and negative externalities can arise in digital markets, in addition to the direct tradeoffs implicated by a person's decisions about information sharing. For example, external benefits and harms may arise when individuals choose to share information, because the information can be used as inputs in processes that determine the quality and rating of, and extent to which, products and services are available to others. Third parties, and aggregate social welfare may also be harmed (or forgo efficiencies) when information about certain conduct or attributes (e.g., insider trading, communicable diseases, loan defaults) is hidden, or access to it is restricted or otherwise impeded; contrariwise, third parties or aggregate social welfare may benefit when other types of information are suppressed (e.g., juvenile criminal records)[50] or, in the alternative, collected and shared. For instance, the aggregation of online searches may unveil unexpected interactions between pharmaceutical drugs,[51] provide early alerts for epidemics,[52] or facilitate contact tracing to control the spread of infectious diseases, such as COVID-19.[53] Conversely, the

---

[47] Secretary, U.S. Dep't Housing & Urban Dev. V. Facebook, Inc., FHEO No. 01-18-0323-8, 3 (2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

[48] *Id.* at 4-5.

[49] A ride-sharing service, for instance, may charge users or offer them promotional pricing differently based on their individual usage habits, which may result in higher or lower prices for users depending, e.g., on their estimated demand elasticity for a particular ride at a particular time and whether or not they also tend to utilize and compare rates with a competing service.

[50] We present this as an example of information suppression that is widely considered beneficial (and, not incidentally, in many instances required by law). We do not suppose that assessment to be universally shared or precisely measured.

[51] Ryen W. White, et al., *Web-scale Pharmacovigilance: Listening to Signals from the Crowd*, 20 J. AM. MED. INFORMATICS ASS'N 404 (2013) (results suggesting logs of the search activities of populations of computer users can contribute to drug safety surveillance.

[52] *See, e.g.*, Andrea Freyer Dugas, et al., *Google Flu Trends: Correlation with Emergency Department Influenza Rates and Crowding Metrics*, 54 CLINICAL INFECTIOUS DISEASES 463 (2012); Ryen W White, et al., *Web-Scale Pharmacovigilance: Listening to Signals from the Crowd*, 20 J. AM. MEDICAL INFORMATICS ASSOC. 404 (2013).

[53] *See, e.g.*, David O. Argente, et al., *The Cost of Privacy: Welfare Effect of the Disclosure of COVID-19 Cases*, NBER Working Paper 2270 (May 2020), http://www.nber.org/papers/w27220 (using detailed mobile data and estimating that change in commuting patterns due to public disclosure lowers the number of cases by 400 thousand and the number of deaths by 13 thousand in Seoul over two years.); Prime Minister Australia,

practice of sharing data, by those willing to do so, could legitimize the continuation or expansion of processes or conduct that other people may find intrusive.[54]

Similarly, a consumer may benefit from other people's information sharing : consider, e.g., product, service, movie, and music ratings and reviews – or, further, access to medical treatment informed by evidence-based treatment guidelines.[55] Conversely, because information regarding similar third-persons can facilitate inferences about a first person, a consumer may pay a price when data (and analytics) permit a seller to accurately predict how much that person values a product. That is, one's ability to maintain, as private, certain information about oneself may depend on privacy choices made by others.[56]

As discussed below, direct and indirect benefits, as well as direct and indirect costs, may vary across the population; and the valuation of those benefits and costs may be relatively straightforward or relatively complex, both for individual consumers and across the population of consumers.[57]

This is a complex subject, and the complexity begins with the underlying subject matter: Privacy has been variously defined, often from outside the field of economics, and often in terms that do not readily map to technical or policy choices. Warren and Brandeis famously provide an extended meditation on privacy as a "right to be let alone" that, in their estimation, was distinct from extant rights in property or others protected by the

---

COVIDSAFE: New App to Slow the Spread of Coronavirus (Apr. 2020), https://www.pm.gov.au/media/covidsafe-new-app-slow-spread-coronavirus (announcing mobile app and recommending its download and use by all Australians); Laura Bradford, et al., *COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes*, J. LAW AND THE BIOSCIENCES (2020), https://doi.org/10.1093/jlb/lsaa034. (noting role of digital contact tracing in reducing spread of pandemic in China, Israel, Singapore, and South Korea, and discussing issues posed by new interfaces for Android and Apple devices). Cf. Ctrs. for Disease Control and Prevention (CDC), Contact Tracing (updated Jun. 21, 2020), https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/contact-tracing.html.

[54] *See, e.g.*, Jay Pil Choi, et al., *Privacy and Personal Data Collection with Information Externalities*, 173 J. PUB. ECON. 113 (2019); Daron Acemoglu, et. al, *Too Much Data: Prices and Inefficiencies in Data Markets*, NBER Working Paper No. 26296 (Sept. 2019), https://www.nber.org/papers/w26296.

[55] *See, e.g.*, Beatrice Fervers, et al., *Predictors of High Quality Clinical Practice Guidelines: Examples in Oncology*, 17 INT. J. QUALITY HEALTH CARE 123 (2005). Such benefits may be substantial, especially with rigorously developed clinical practice guidelines, although the development of effective clinical practice guidelines is not without challenges. *See id.*; Inst. of Med., Clinical Practice Guidelines We Can Trust, ch. 3 (2011).

[56] That is, such information can improve the quality of information about a class of people; and readily (or otherwise) available information may identify an individual with the class.

[57] *See* text accompanying notes 95-109, *infra*; *see also* Brynjolfsson, Collis, and Eggers, supra note 32.

common law, although having roots or analogs in several of them.[58] The "right" they described was not a well-developed theory of privacy, or privacy protections; rather, they set out certain guideposts for what they anticipated – or hoped – would be the common law development of a "right to be let alone," which would emerge from courts' evaluations of various tradeoffs according to the facts and circumstances of numerous particular disputes.[59]

Among its other definitions, privacy has been described as an aspect or foundational element of dignity and autonomy,[60] and as the control over and the safeguard of personal information by the subject of that information.[61] It pertains to the boundaries between what is personal and that which is more widely shared,[62] and the decisions one can and may choose to make about those boundaries. Those decisions may entail complex tradeoffs concerning benefits and costs that are both tangible and intangible, under varying conditions of uncertainty, and with effects on others that may vary along a number of dimensions. Prosser, while not claiming to offer a precise definition of privacy, identified four "rather definite" privacy rights: Intrusion upon a person's seclusion, solitude, or private affairs; public disclosure of embarrassing private facts about an individual; publicity placing one in a false light in the public eye; and appropriation of one's likeness for the advantage of another.[63] Solove reviewed six broad categories of conceptions of (or perspectives on) privacy: "(1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy."[64] Noting

---

[58] *See generally*, Warren & Brandeis, *supra* note 39 (citing THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT (1879)).

[59] *Id.* at 214-215.

[60] FERDINAND SCHOEMAN, PRIVACY AND SOCIAL FREEDOM (1994).

[61] ALAN F. WESTIN, PRIVACY AND FREEDOM, (1967).

[62] *See* IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975).

[63] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

[64] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1088, 1094 (2002); *see also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477 (2006) ("Many commentators have spoken of privacy as a unitary concept with a uniform value, which is unvarying across different situations. In contrast, I have argued that privacy violations involve a variety of types of harmful or problematic activities." Id. at 480).

difficulties with each of them, he suggested a "pragmatic" and context dependent approach rather than a particular theory or model.[65]

Additional candidates are numerous and varied, as are rejections of the promise of a simple unified theory of privacy.[66] We note the diversity of these threads to inform, rather than undermine, understanding of both the economic study of privacy and its application to policy; areas of interest or concern may be many and diverse, but that does not gainsay their importance.

Economic research on personal privacy has primarily focused on the collection and flow of information, including the tradeoffs arising from the sharing or withholding (or even suppression) of personal data.[67] As explained below, we note that this economic focus dovetails with the larger body of FTC enforcement actions regarding both privacy and data security under both the deception and unfairness prongs of Section 5 of the FTC Act.[68] We note, too, that economics comprises a diverse body of research pertinent to privacy and data security that, while interrelated, does not stem from a consensus theory or definition of privacy. That may be a feature rather than a bug: if a general theory of privacy is supposed to inform policy, settling on a general theory prior to significant economic inquiry into the implications of various policy choices, made in various market contexts, is

---

[65] *Id*. at 1116–17.

[66] *See* notes 56 - 63, *supra*, and accompanying text; *see also*, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015). The philosopher Judith Jarvis Thompson has said, "[p]erhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is." Judith Jarvis Thomson, *The Right to Privacy*, 5 PHILOSOPHY AND PUBLIC AFFAIRS 295, 295 (1975).

[67] Posner (1978, 1981, 1993) and Stigler (1980), for instance, argued that establishing protected classes of information can create inefficiencies in the marketplace, since doing so conceals potentially relevant information from other market participants, and that market participants may seek ways around such restrictions. Richard A. Posner, *Blackmail, Privacy, and Freedom of Contract*, 141 U. PA. L. REV. 1817 (1993); Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405 (1981); Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393 (1978); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623 1980. For instance, in matching employees with employers, the protection of (positive or negative) information about potential employees can come at the cost of suboptimal matching, and employees with positive information will seek ways to signal it. Hirshleifer argued, however, that markets may suffer from over-collection of personal information. Jack Hirshleifer, *Privacy: Its Origin, Function, and Future*, 9 J. LEGAL STUD. 649 (1980). For instance, competition among banks to offer better borrowing rates may lead to a suboptimal level of data collection. Jeremy M. Burke, Curtis R. Taylor, & Liad Wagman, *Information Acquisition in Competitive Markets: An Application to the US Mortgage Market*, 4 AM. ECON. J.: MICROECONOMICS 65 (2012).

[68] *See* text accompanying notes 185–111, pp. 25-27, *infra*.

not obviously the best order of operations. Economic analysis of privacy—and of privacy policies or regulations—has led to conclusions that may vary depending on the market, time, and individuals concerned, in part because of the interface of privacy and other policy objectives, such as competition.[69]

In practice, people also tend to be imperfectly informed about both the sharing of personal information and its potential consequences,[70] and specific disclosures, whether accurate or inaccurate, may influence their privacy decisions.[71] That is, for individuals, information *about* the tradeoffs implicated in sharing or withholding personal information may not be readily available and may ultimately be imperfect and costly to acquire. Such information costs can be asymmetric as well; that is, potentially more costly for consumers than for the firms who collect such information.

The benefits of privacy – and certain privacy protections – may sometimes appear clear. For example, anyone might be concerned about identity theft, and there might also be widespread agreement that spam calls and revenge porn are harmful, and ought to be restricted.[72] However, in economic terms, it has not been possible to generally and unambiguously conclude that increasing privacy protections always entails net gains in consumer surplus or social welfare. It is understood that privacy decisions, including

---

[69] *See, e.g.*, Curtis Taylor & Liad Wagman, *Consumer Privacy in Oligopolistic Markets: Winners, Losers, and Welfare*, 34 INT'L J. INDUS. ORG. 80 (2014), for examples of how different economic models can lead to positive or negative privacy consequences. *See* Idris Adjerid et al., *The Impact of Privacy Regulation and Technology Incentives: The Case of Health Information Exchanges*, 62 MGMT. SCI. 104 (2016), for an example of how different attributes of privacy laws can lead to both positive and negative effects from privacy-related regulation.

[70] *See, e.g.*, Hana Habib, et al., *Away from Prying Eyes: Analyzing Usage and Understanding of Private Browsing,* 18th Symp. on Usable Privacy & Sec. (SOUPS 2018) 159 (2018), https://www.usenix.org/system/files/conference/soups2018/soups2018-habib-prying.pdf; Pedro G. Leon, et al., What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers, Proc. of the Eighth Symp. on Usable Privacy & Sec. (SOUPS '13) (2013), http://cups.cs.cmu.edu/soups/2013/proceedings/a7_Leon.pdf; Lorrie F. Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH L. 273 (2012).

[71] *See, e.g.*, Idris Adjerid, Alessandro Acquisti, & George Loewenstein, *Choice Architecture, Framing, and Cascaded Privacy Choices*, 65 MGMT. SCI. 1949 (2019), for an experiment in which participants' choice of privacy settings significantly influenced disclosure choices, as well as where individuals' downstream behaviors do not adjust as a function of their privacy settings. *See also* Arunesh Mathur, et al., *Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites*, 3 Proc. ACM Human-Computer Interaction Art. 81, CSCW (2019), https://arxiv.org/pdf/1907.07032.pdf, for an example of how "dark patterns" may be used to elicit consumer consent for information sharing.

[72] *See* text accompanying notes 198 - 200, *infra*, regarding FTC enforcement examples.

decisions about privacy policies, can involve tradeoffs—for instance, ensuring the privacy of a consumer's purchases may protect them from price discrimination (supposing the reserve price is lower than a uniform market price), but deny them the potential benefits of targeted discounts and other offers. Such trade-offs are common even before considering unintended effects, or the relative efficacy or efficiency of any given policy intervention.

b. A Brief Overview of Privacy-Related Law[73]

The central but not exclusive statutory basis of FTC privacy enforcement has been Section 5 of the FTC Act, which generally prohibits both "unfair methods of competition" and "unfair or deceptive acts or practices in or affecting commerce."[74] "Unfair or deceptive acts or practices" (often referenced as "UDAP") —the consumer protection prong of the FTC Act—provides the basis for the large body of the FTC's privacy actions, [75] although both commentators and the Commission itself have considered whether "unfair methods of competition – the antitrust prong – should apply as well.[76] There is no express charge to regulate either privacy or data security under the FTC Act. There have been numerous applications of the FTC's "unfair or deceptive acts or practices" ("UDAP") authority to privacy-related issues. For example, material misrepresentations of a firm's privacy

[73] This is a brief overview of a complex space. Extant federal and state legal requirements pertaining to data privacy (statutes, regulations, and judicial decisions) are numerous. We make no attempt to list all of them., although we do mean to sketch central examples.

[74] 15 U.S.C. § 45(a)(1).

[75] Although mainly focused on privacy research, we note that privacy and data security concerns, research, and regulation, can overlap in various ways. For that reason, we sometimes use "privacy" as a shorthand for privacy and data security.

[76] *Compare, e.g.*, Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769 (2010) (suggesting possible antitrust actions regarding privacy) *with* Maureen K. Ohlhausen and Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L. J. 121 (2015) (suggesting that most privacy issues are not well suited to antitrust law). The FTC's 2022, ANPR raises two questions about the potential impact of data regulations on competition, *supra* note 2, at 5182-83, and two about potential *harm* to competition stemming from commercial data practices, *id.* at 51283-843.

policies or performance could be actionable deceptive acts.[77] And substandard security alleged to expose sensitive consumer data might be deemed unfair.[78]

At the same time, there are federal and state statutes that address privacy and data security concerns expressly. The other federal laws have more limited reach than the FTC Act, with most of them focusing on industry- or domain-specific data. Several of these more specific laws are enforced by the FTC itself, including the Children's Online Privacy Protection Act of 1998 (COPPA),[79] which restricts collection and use of personal information collected from children under the age of thirteen, the Financial Services Modernization Act of 1996 (Gramm-Leach-Bliley Act or GLB),[80] which regulates the use and dissemination of consumers' "nonpublic personal information" by "financial institutions," broadly defined, the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM),[81] which enables consumers to opt-out of receiving certain types of commercial e-mail, and the Telemarketing and Consumer Fraud and Abuse Prevention Act,[82] which provided the FTC with the authority used to adopt the Do Not Call Registry.[83] The FTC also shares enforcement responsibility with the Consumer Financial Protection Bureau for the Fair Credit Reporting Act (FCRA),[84] which sets out requirements for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants.

---

[77] *See, e.g.*, In the Matter of Ortho-Clinical Diagnostics, Inc., FTC Docket No. C-4723 (2020), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3050-ortho-clinical-diagnostics-inc-matter.

[78] *See, e.g.,* In the Matter of Uber Technologies, Inc., FTC Docket No. C-4662 (2018) (revised complaint alleging both unfairness and deception), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3054-c-4662-uber-technologies-inc-matter.

[79] 15 U.S.C. §§ 6501-6506.

[80] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.)

[81] 15 U.S.C. §§ 7701- 7713.

[82] 15 U.S.C. §§ 6101- 6108.

[83] 16 CFR part 310.

[84] 15 U.S.C. §§ 1681-1681x. Initially, the FTC had sole enforcement authority for the FCRA. It retains some of that authority under the FCRA, 15 U.S.C. § 1681s(a)(1); but Congress has taken steps to augment and partition that enforcement authority via amendments, providing for, *e.g.*, actions brought by state attorneys general in 1987, 15 U.S.C. § 1681s(c), and assigning considerable regulatory authority to the Consumer Financial Protection Board as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act. Pub. L. 111-203, 111th Cong. (Jul. 21, 2010). Title X of the Act, § 1001 et seq., establishes the CFPB, with FCRA enforcement authority codified at 15 U.S.C. § 1681s(b)(1)(H).

The Department of Education enforces the Family Educational Rights and Privacy Act (FERPA),[85] which provides access to and some control over student records for a student or her parents, depending on the student's age. And the Department of Health and Human Services enforces the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[86] which protects the privacy and security of health information, although it refers certain HIPAA cases to the Department of Justice for criminal prosecution.[87] It should be noted that some HIPAA violations may also be deemed violations of the FTC Act.[88]

We also note new cyber security regulations adopted by the SEC that add substantially to established disclosure obligations under the Securities Exchange Act of 1934 (SEC Act).[89] The new rules "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, ad incidents by public companies" subject to reporting requirements under the SEC Act.[90] The rules also require "periodic disclosures about a registrant's process to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity

---

[85] 20 U.S.C. § 1232g; 34 CFR Part 99

[86] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, as amended (codified at 42 USC §§ 1320d et seq.). Implementing regulations, the HIPAA privacy, security, and enforcement rules, are at 45 CFR Parts 160 and 164.

[87] See, e.g., Dep't Health & Human Servs., Health Information Privacy, Enforcement Highlights, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html. noting that HHS had investigated and resolved more than 29,000 HIPAA privacy rule cases through December 2022, in addition to referring 1,640 matters to the Department of Justice for criminal investigation).

[88] For example, in 2008, the FTC and the Department of Health and Human Services both settled charges regarding the same underlying course of conduct by CVS Caremark. The FTC had alleged that the firm failed to take reasonable and appropriate measures to protect consumers' sensitive health and financial information, in violation of the FTC Act, while the Department of Health and Human Services had alleged violations of the Health Insurance Portability and Accountability Act (HIPAA). Fed. Trade Comm'n, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations, Feb. 18, 2008, https://www.ftc.gov/news-events/news/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial-privacy-customers-employeescvs. *See, e.g.*, Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case, Dep't Health & Human Servs. (2017) (regarding coordinated investigation of alleged HIPAA privacy rule violation and alleged FTC Act by HHS and FTC), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/rite-aid/index.html#_content-order; In the Matter of Rite Aid Corp., FTC Docket No. C-4308 (2022) (FTC final decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaiddo.pdf.

[89] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896 (Aug. 4, 2023) (final rule) (to be codified at 17 C.F.R. Parts 229, 232, 239, 240, and 249).

[90] *Id.* at 51896.

risks, and the board of directors' oversight of cybersecurity risks."[91] While these rules do not apply to all persons "in commerce," they do apply to "[e]very issuer which is engaged in interstate commerce or in a business affecting interstate commerce, or whose securities are traded by use of the mails or any means or instrumentality of interstate commerce" if the issuer "has total assets exceeding $10,000,000 and a class of equity security (other than an exempted security held of record by either (i) 2,000 persons or (ii) 500 persons who are not accredited investors."[92] That is, the rules apply at least to all publicly traded firms.

State privacy laws are numerous, and comprise both wide ranging statutes, such as the California Consumer Privacy Act of 2018,[93] and laws of narrower application, such as the Delaware statute prohibiting the marketing of certain products and services to children on websites, computing services, and online or mobile applications.[94] There is, as well, a body of state common law regarding privacy matters.[95]

Finally, there are numerous data privacy restrictions that have been adopted and enforced by non-U.S. authorities. We note that the European Union's General Data Protection Regulation ("GDPR"), and its implementation by various national authorities,[96] is of interest for at least several reasons.[97] For one, GDPR's reach over EU member states

---

[91] *Id.*

[92] 15 U.S.C. § 781(g); see also id. at 781(b) for procedures for registering firms on a national securities exchange.

[93] Cal. Civ. Code Div. 3, Pt. 4, Title 1.81.5

[94] Del. Code § 1204(C). For an overview of general and specific state privacy laws, see, e.g., NCSL Nat'l Council of State Legislatures, State Laws Related to Digital Privacy, https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (3/11/2021).

[95] *Compare, e.g.,*, Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law, a Mixed Legacy*, 98 CAL. L. REV. 1887 (2010), *with* William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960); RESTATEMENT (SECOND) OF TORTS (1965).

[96] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), which became effective in 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. GDPR is subject to implementation and enforcement by national authorities of the EU member states. For example, German implementation of GDPR is found in Bundesdatenschutzgesetz, Neufassung 2018 ("BDSG") and amendments to numerous prior laws.

[97] For a review of research specifically related to GDPR, see Garrett A. Johnson, *Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond* in THE ECONOMICS OF PRIVACY (eds. Avi Goldfarb & Catherine Tucker) (forthcoming), https://ssrn.com/abstract=4290849.

(and effective persistence in the United Kingdom since Brexit)[98] is a matter of significant economic import. Second, GDPR is an example of the sort of law absent at the national level in the U.S. and certain other jurisdictions; that is, as its name suggests, a General Data Protection Regulation, ranging over both privacy and data security issues across industries and categories of consumer data. Not incidentally, it is often discussed as a potential model for privacy regulation in the U.S. and elsewhere.[99] Third, as outlined below, the relatively recent implementation of the GDPR – adopted in 2016 and effective in 2018 – has provided a timely and significant regulatory event for empirical investigation, both sufficiently recent and sufficiently established to provide an instructive comparison or control for contemporary policy discussion; to some extent, the results of those studies may be generalized to other privacy regimes. And fourth, GDPR has a direct bearing on international data flows involving the EU region as well as EU persons, and, hence, on numerous firms and a significant tranche of data-related commerce beyond the EU.

II. The Economics of Privacy

a. High-Level Observations on Privacy as an Economic Good

Privacy and personal information have multiple economic characteristics. When shared, information can be copied or replicated, so that its use by one party does not necessarily impinge on or exclude repeat or rival usage by another.[100] Information – and analogous goods – are thus said to be "non-rivalrous." Partly because information is non-

---

[98] Although the UK has withdrawn from the EU, its implementation of GDPR have, in large part, been maintained via the Data Protection Act of 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted, and the UK General Data Protection Regulation, which became effective in 2021, https://www.legislation.gov.uk/eur/2016/679/contents.

[99] See, e.g., Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy,* 123 YALE L. J. 266 (2013-14) (based on pre-adoption draft of GDPR); Caitlin Chin, Highlights: The GDPR and CCPA as Benchmarks for Federal Privacy Legislation, Brookings Inst. (2019), https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/. The FTC's advance notice discusses GDPR as an example, ANPR at 51278, and expressly asks whether the Commission "should take into account other governments' requirements as to data security (e.g., GDPR)? If so, how?" ANPR at 51282.

[100] Anja Lambrecht & Catherine Tucker, Can Big Data Protect a Firm from Competition, CPI Antitrust Chronicle (2017), https://www.competitionpolicyinternational.com/wp-content/uploads/2017/01/CPI-Lambrecht-Tucker.pdf.

rivalrous (or, at least, susceptible to copying and dissemination at relatively low cost), complex digital ecosystems tend to engage in complex trades of information; once data are released, it can be difficult to prevent their duplication as well as their access by third parties, and it can be difficult to prevent their downstream uses, which themselves are difficult to predict or trace. At the same time, one of the core tenets of privacy is the ability to limit access to information.

Privacy interests, preferences, practices, and policies often entail tradeoffs of benefits and costs. The values of keeping personal information private and of sharing it can be heterogeneous across individuals, almost entirely context dependent, and changeable over time.[101] Consumer harms in privacy matters – or "informational injury" – may be diverse.[102] For any given consumer, a firm's data practices may implicate both benefits and harms.[103] And the magnitudes of such benefits and harms may vary across consumers, such that practices or policies may implicate the distribution of costs and benefits to consumers in the market, and not just the net aggregate of costs and benefits.[104] Further, the costs and benefits of sharing and collecting information may be asymmetric for consumers and firms; and the extent of saliency – the prominence, availability, and the cost of internalizing

---

[101] A healthy individual who just lost his job may flaunt his active lifestyle on social media, but hide his unemployment status to avoid shame; the reverse may be true for the affluent manager who was just diagnosed with a sexually-transmitted disease. *See* Acquisti, Taylor, & Wagman, *supra* note 24; HELEN NISSENBAUM, PRIVACY IN CONTEXT (2009).

[102] *See generally, e.g.,* Fed. Trade Comm'n, FTC Informational Injury Workshop: BE & BCP Staff Perspective (2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf; Acquisti, Taylor & Wagman, *supra* note 24 ("at its core, the economics of privacy concerns the trade-offs associated with the balancing of public and private spheres between individuals, organizations, and governments." *Id.* at 444); Leslie K. John, Alessandro Acquisti & George Loewenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. CONSUMER RES. 858 (2011).

[103] *See, e.g.*, text accompanying note 30, *supra*; Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509, 509-10 (2015).

[104] *See, e.g.*, Acquisti, Taylor, and Wagman, supra note 24, at 4-5; see also, e.g., Curtis Taylor & Liad Wagman, *Consumer Privacy in Oligopolistic Markets: Winners, Losers, and Welfare*, 34 INT'L J. INDUS. ORG. 80 (2014); Jeremy M. Burke, Curtis R. Taylor, & Liad Wagman, *Information Acquisition in Competitive Markets: An Application to the US Mortgage Market*, 4 AM. ECON. J.: MICROECONOMICS 65 (2012) (finding, in mortgage markets, that firms' "ability to sell consumer information leads to lower prices, higher screening intensities, higher rejection rates, and, perhaps more importantly, increased ex-ante social welfare."); Omri Ben-Shahar, *Data Pollution*, 11 J. LEG. ANALYSIS 104 (2019) (regarding negative externalities or spillover effects in privacy); Ginger Zhe Jin & Andrew Stivers, *Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics*, SSRN Working Paper (May 22, 2017), http://dx.doi.org/10.2139/ssrn.3006172.

information about such costs and benefits – may be asymmetric as well. For service providers, data can be the essence of a transaction (e.g., as with a search engine or a mapping service), whereas for users, downstream trade of personal data can be a secondary and less salient aspect of the experience (where the user is focused on, e.g., searching for the nearest doctor or posting on social media). Potential downstream uses and associated risks can often be opaque.

For consumers, privacy tradeoffs – privacy-related benefits and harms or costs – often mix attributes that are more and less observable, or that avail themselves to different degrees of measurement and ordering (e.g., tangible factors, such as applying a coupon or the imposition or waiver of an access fee, and intangible factors, such as the discomfort experienced when something personal is shared without the subject's consent). We note that current difficulties in observation, measurement, and ordering have implications for policy and enforcement, but are not necessarily intractable or permanent. Pappalardo, for instance, suggests that some of the limitations of the assessment toolkit may be due to the relatively underdeveloped literature on the economics of consumer protection.[105]At the same time, a former FTC consumer protection practitioner, Pappalardo, points to positive contributions of FTC economists, through a combination of research, case evaluation, and policy analysis, to the definition and estimation of consumer harms or injuries from deceptive or unfair practices, including those associated with lapses in data security or privacy protections.[106] She also describes a framework for estimating injury from

[105] Janis K. Pappalardo, *Economics of Consumer Protection: Contributions and Challenges in Estimating Consumer Injury and Evaluating Consumer Protection Policy* (forthcoming in J. CONSUMER POL'Y 2020).

[106] Published material from the FTC's Bureau of Economics, for example, outlines an approach to assessing consumer harm in matters such as *Wyndham*, where the FTC alleged both direct financial losses and time spent to remedy those losses and guard against future ones. The approach takes into account the estimated baseline rate of identity theft, conditional on a consumer's being subject to a breach. And, because the Section 5 violation was predicated on the firm's deceptive statements, FTC Bureau of Economics staff also estimated the price premium that consumers paid due to those deceptive statements, multiplied by an estimate of the number of consumers affected. See Dan Hanner, Ginger Zhe Jin, Marc Luppino & Ted Rosenbaum, *Economics at the FTC: Horizontal Mergers and Data Security*, 49 REV. INDUS. ORG. 613 (2016) (section on estimating harm from data breaches with application to *Wyndham* at 627 – 630).

deception using a combination of methods, such as consumer copy testing and comparative demand analysis, that have been applied in such matters.[107]

Consumer copy testing comprises various randomized controlled experiments designed to measure the effect of a potentially (or allegedly) misleading claim on consumers; that is, the question whether a claim is misleading and, if so, to what extent.[108] Comparative demand analysis then seeks to model the effect of false or misleading claims on consumer demand, comparing the demand shift associated with the provision of materially false or misleading information (or, potentially, the omission of certain material information) with a counterfactual. Although sometimes treated as a comparison between demand under conditions of perfect information and degraded information (regarded by Pappalardo, among others, as an impractical comparison), it can also be used to examine the demand shift from some baseline demand associated with non-misleading information to that associated with a particular instance of false or misleading information.[109]

Pappalardo links these approaches to harms associated with marketing practices (e.g., for the purpose of estimating injury arising from materially false or misleading claims about a firm's data policies and practices). Not incidentally, many of the FTC's privacy enforcement actions are rooted in the Commission's Section 5 authority regarding deceptive acts or practices in commerce. There may, of course, be many harms or informational injuries that have no straightforward connection to deceptive advertising or marketing practices.

Privacy may also be valued or evaluated either instrumentally or in its own right. In the alternative, it might be evaluated as a process or an outcome. That is, privacy may have

---

[107] Pappalardo further describes how comparative demand analysis can be applied to model legal concepts of either expectation or reliance damages and, building on Hunter, et al., to provide an analysis consistent with the construct of reliance damages. *Id.* (citing John Hunter, et al., *Measuring Consumer Detriment Under Conditions of Imperfect Information*, Off. Fair Trading, UK (2001)).

[108] Pappalardo discusses some of the issues involved in constructing a controlled copy test. See *id.* at draft 17-18; *see also* Richard Craswell, *Compared to What?' The Use of Control Ads in Deceptive Advertising Litigation*, 65 ANTITRUST L.J., 757 (1997); Janis K. Pappalardo, *The Role of Consumer Research in Evaluating Deception: An Economist's Perspective*, 65 ANTITRUST L.J. 793 (1997).

[109] *Compare, e.g.*, Pappalardo (forthcoming) *with* John Hunter, et al., *Measuring Consumer Detriment Under Conditions of Imperfect Information*, Off. Fair Trading, UK (2001) (considering consumer "detriment" as the loss in consumer surplus associated with the demand shift, and sketching various techniques to measure the detriment, depending on the available data).

aspects of an "intermediate good," a "final good," or both.[110] For example, an individual may consider his or her privacy when deciding whether to set a social media profile as private or public, but may or may not recognize or consider the increased risk of identity theft or inadvertent privacy intrusion when adding a friend or family member as a direct connection on their social media account.[111] Moreover, the reference points associated with the value of privacy are unclear. For example, should the reference point be the price one would accept to surrender the data in question (willingness to accept, or WTA), which is potentially associated with an endowment effect, or the price one would pay to protect it (willingness to pay, or WTP)? Should it be the anticipated costs consumers may suffer if their information is exposed, or the profit a seller can generate from acquiring the information?[112]

For all of these reasons, the assessment of privacy harms, and determinations of net harm, may sometimes be challenging. That is, whereas some privacy harms can be straightforwardly measured, others may be difficult to measure or assess systematically. For example, the financial costs associated with identity theft may be discoverable in specific cases or known on average; that is, more-or-less discoverable, if incompletely so.[113] Other harms, such as the disquiet many consumers may feel when strangers become aware of their personal information, can – lacking market valuation or any established or straightforward market proxy – be more difficult to measure or estimate. Correspondingly, the valuation of privacy harms caused by a given practice or course of conduct can be multilayered. For instance, the failure to implement reasonable practices to safeguard

---

[110] Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. TELECOMM. HIGH TECH. L. 251 (2012).

[111] A consumer might view the ability to grant (or not grant) an individual human person—or a larger set of them—access to his or her posted material on a social network as a direct informational benefit, analogous to a final good. A consumer might also (or alternatively) value that ability because he or she is concerned about downstream risks, such as greater susceptibility to malicious actors and harmful conduct, such as identity theft, which could increase with a larger network. A consumer might also have limited knowledge about those downstream uses, and about the risks associated with them.

[112] *See, e.g*, A. Mitchell Polinsky & Steven Shavell, *Should Liability Be Based on the Harm to the Victim or the Gain to the Injurer?*, 10 J.L. Econ. & Org. 427 (1994).

[113] See, e.g., FTC v. Wyndham Worldwide Corp., notes 108, 191-192, *infra*, and accompanying text (harms including financial losses, among others, to lenders and end-consumers via credit card theft); see also, Langton Testimony, FTC Informational Injury Workshop, *supra* note 9, transcript pp. 214-17 (regarding National Crime Victimization Survey, and reporting, e.g., average risk of identity theft conditional on breach and variety of associated harms, including financial and others).

sensitive information may be deemed unfair, particularly when it leads to a breach and demonstrable or likely harm.[114]

At the same time, assessing the diminution of data risk or the expected harm from the adoption and implementation of particular privacy policies or lack thereof may require a deeper inquiry.[115] Economic harms are not merely financial ones, or those subject to trivial or canonical measurement. That harms may be various, estimated with greater or lesser precision, and with varying degrees of confidence is not unique to the topic of privacy. Still, identification and measurement difficulties in this space are many, and they can often entail modeling or measuring some considerations and not others.

b. A Note on Information Costs and Rational Ignorance:

There is research indicating that many consumers do not read the privacy policies posted by firms and other organizations, and that many who do fail to comprehend those policies.[116] That may suggest a problem for many consumers, if one that further disclosure research and consumer education might ameliorate to some extent; and it may also pose a problem for certain regulatory interventions. Still, there is an open question regarding what such policy information is worth to any given consumer. Beales and Muris recognize that some consumers value privacy – and perhaps, privacy policies – greatly, while others

---

[114] In addition, misrepresentations regarding such policies may violate Section 5 of the FTC Act. *See, e.g.*, Fed. Trade Comm'n, FTC Files Complaint against Wyndham Hotels for Failure to Protect Consumers' Personal Information (2012), https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect; FTC v. Wyndham Worldwide Corp. et al., Civil No. 13-1887 (D.N.J. Apr. 7, 2014) (opinion denying defendant's motion to dismiss); 799 F.3d 236 (3d Cir. 2015).

[115] *See, e.g.*, Sasha Romanosky, et al., *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1 (2019) (reviewing 235 selected filing dockets, from large and small underwriters, from 2007-20017, and finding that "the first and most important firm characteristic used to compute insurance premiums was the firm's asset value (or revenue) base rate, rather than specific technology or governance controls." *Id.* at 17.)

[116] Regarding the readability of privacy policies, see, e.g., Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S J. of L. & Pol'y for Info. Society 543 (2008); Mark A. Graber, et al., *Reading Level of Privacy Policies on Internet Health Web Sites*, 51 J. FAMILY PRACTICE 642 (2002); Ali Sunyaev, et al., *Availability and Quality of Mobile Health App Privacy Policies*, 50 J. Amer. Med. Informatics Assn. 28 (2014). *But see* Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEG. STUD. S69 (2016) (experimental evidence that many consumers can comprehend sample privacy policies).

do not.[117] They note that for many, a failure to digest complex privacy policies may reflect "rational ignorance":

> Consumers ... maintain rational information about how much and what kind of information sharing occurs. It simply does not pay for most consumers to think and make decisions about policies on the use of their information, given that the issue is of such little practical consequence to them.[118]

Different factors may be at play for different consumers. Consider the relationships between a privacy policy as written, a privacy policy as implemented or observed by a firm, and the risk of material harm (some function of the likelihood and magnitude of harms a given consumer considers material). A consumer might attach low value to reading and comprehending a privacy policy because the consumer attaches little value to privacy generally, or because they doubt that the policy will address their individual privacy concerns or priorities. Or they might doubt the nexus between the policy and their risk of harm, perhaps because they doubt the efficacy of such policies. In any case, they may doubt that the marginal benefit of search will exceed the marginal cost.

Both private litigants and enforcement agencies may face difficulty in seeking to establish a causal link, or "proximate" cause, where there are demonstrable consumer harms. As noted above, risk-assessment experts have found it extremely difficult to assess or price risk according to variation in firm privacy policies.[119] Even privacy-sensitive consumers may reasonably question the marginal benefit – such as the marginal

---

[117] J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHICAGO L. REV. 109, 115 (2008). *See also* James C. Cooper & Joshua Wright, *The Missing Role of Economics in FTC Privacy Policy*, in CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Jules Polonetsky, Evan Selinger & Omer Tene, eds.) (2017).

[118] *Id.* at 115.

[119] Research by Romanosky, *et al.,* suggests some of the challenges of risk assessment. Sasha Romanosky, *et al.*, *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1 (2019) (reviewing 235 selected filing dockets, from large and small underwriters, from 2007-20017, and finding that "the first and most important firm characteristic used to compute insurance premiums was the firm's asset value (or revenue) base rate, rather than specific technology or governance controls." *Id.* at 17.)

diminution of risk – they are likely to derive from any particular change in a firm's privacy policies.

We suggest that policy makers and expert agencies may face analogous problems. That is, given the heterogeneity of privacy preferences, the complexity of tradeoffs potentially entailed by privacy policies, and uncertainty about the likely risk management potential of a given possible policy change, it may be difficult to justify on a cost-benefit basis the value of a proposal to require one policy or another.

c. Recent Lessons from Privacy Economics

Privacy research comprises diverse methods and subjects, and it includes both theoretical and empirical studies. Empirical research ranges over, *inter alia*, consumer behavior, knowledge, and preferences; commercial policies and practices; public policies (including laws and regulations); and the intersection or interaction among subsets of these phenomena. We focus, here, on a sample of empirical research regarding the effects of public policies. Such economic effects include, but are not limited to, those typically tallied or estimated in cost-benefit analyses. We note, at the outset, that formal (and often required) government-conducted cost-benefit analyses are commonly and variously bounded exercises, and that they often eschew attempts to estimate, among other things, the impact of laws and regulations on competition and innovation. We also reiterate, as a significant potential limitation, a paucity of research regarding the benefits of privacy regulations. Following are brief summaries of a subset of recent empirical work in which researchers evaluate some of the effects of different privacy protection rulesets. These works highlight a few over-arching observations. First, each dimension of privacy protection tends to fall on a spectrum, and moving from one point to another on this spectrum may entail diverse tradeoffs. Second, these tradeoffs can include spillover effects, including on prices, product or service quality, competition, innovation, and entry.

- **Healthcare**
  - Miller and Tucker, using variations across state medical privacy laws, suggest that certain state privacy regulations (adopted above minimum federal requirements)

that restrict a hospital's release of patient information diminished the adoption of electronic medical records (E.M.R.s), reducing market efficiency in turn. First, they demonstrated local network effects in hospitals' adoption of E.M.R. systems, and found that certain state requirements for patient consent tended to suppress those network effects and, consequently, the rate of E.M.R. adoption.[120] In a second paper, they found that the reduction in efficiency could have a significant impact on certain healthcare outcomes.[121] Miller and Tucker assert that the interaction between data regulations, innovation, and information flow may be complex. For instance, they argue that state-specific regulation may impose costs by increasing regulatory complexity and uncertainty,[122] and that explicit privacy protection could promote the use of information technology by reassuring potential adopters—and their customers—that sensitive information will be protected.[123]

- A study of Health Information Exchanges (HIEs) suggests the potential for certain regulations, in the right contexts, to help promote IT adoption or usage, possibly by reassuring potential adopters. HIEs are information-technology solutions that facilitate

---

[120] Amalia R. Miller & Catherine Tucker, *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records*, 55 MGT. SCI. 1077 (2009). Because both regulation and substantial federal subsidies under, e.g., the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009), have prompted nearly universal adoption of electronic health records systems (EHRs) by U.S. hospitals, there is a question about whether the demonstrated network effect still applies. This was, however, a well-designed study with ongoing relevance to the investigation of, e.g., network effects, spillover, unanticipated, or even perverse effects that may be associated with, or caused by, privacy regulations.

[121] Amalia R. Miller & Catherine E. Tucker, *Can Health Care Information Technology Save Babies?*, 119 J. POL. ECON. 289 (2011).

[122] *See* Miller & Tucker (2009), *supra* note 114. *See also*, text accompanying note 118 - 119, *infra*, regarding Adjerid, et al., *supra* note 67, and Health Information Exchange adoption. For a discussion of complex regulatory impediments, among others, to the adoption of health information technology and the flow of healthcare information, see, e.g., Daniel J. Gilman & James C. Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is Which: Striking The Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279 (2010).

[123] For example, recent OECD publications endorse the notion of fostering consumer trust. *See, e.g.*, the OECD "Going Digital" project: "Trust in digital environments is essential; without it, an important source of economic and social progress will be left unexploited" (https://goingdigital.oecd.org/en/dimension/trust/). *See also* OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation & Companion Doc. (2015) ("calls on the highest level of leadership in government and in public and private organisations to adopt a digital security risk management approach to build trust and take advantage of the open digital environment for economic and social prosperity…"), http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf. *Cf.* OECD, Trust in Peer Platform Markets: Consumer Survey Findings, OECD Digital Econ. Papers No. 263 (2017). https://www.oecd-ilibrary.org/science-and-technology/trust-in-peer-platform-markets_1a893b58-en.

the sharing of patients' electronic medical records among healthcare entities (institutional providers), with the aim of improving the quality and efficiency of care.[124] Their adoption, however, may be hindered by both privacy concerns on the consumer side and privacy laws that restrict the disclosure of health records on the healthcare provider side. Adjerid, et al., compare the formation of HIEs in states with laws that limit information disclosure with states that do not have such laws.[125] They suggest that in their sample, relatively strong privacy policies tend to suppress HIE adoption, but that the combination of adoption subsidies and stronger privacy protections is associated with greater HIE adoption than subsidies, stronger privacy protections, or weaker privacy protections alone. They argue that regulators may find room to balance meaningful privacy protections with incentives for the adoption of new healthcare technologies.

- Miller and Tucker also identify three approaches taken by states to protect patients' genetic privacy with data rights: requiring informed consent; restricting discriminatory usage by employers, healthcare providers or insurance companies; and limited re-disclosure without consent.[126] Their empirical findings suggest that, in their sample, the re-disclosure approach increases the diffusion of genetic testing, in contrast to the informed consent approach, which may deter it.

Although the above studies focus primarily on the potential adoption of new technologies, their results, among others, illustrate some of the tradeoffs that may be implicated by data rights, and may suggest a need to account for, and balance, specific and continually evolving tradeoffs in policy making.

---

[124] Centrally, these are agreements about the sharing of information among providers, although the implementation of such agreements may entail technical and standards endeavors as well.

[125] Idris Adjerid, et al., *supra* note 67. In all cases, such information sharing may be subject to federal and state laws. HIPAA, for example, and its implementing regulations, require patient consent for the release of personal health information, but provide certain exceptions for, e.g., the sharing of information, between providers, for treatment purposes. *See* note 84, *supra*, and accompanying text. The distinction studied, however, turns on the question whether the individual states impose additional express restrictions on the sharing of such information between health care providers, including either an express consent requirement or the combination of a notice requirement and a patient opt-out option.

[126] Amalia R. Miller & Catherine Tucker, *Privacy Protection, Personalized Medicine, and Genetic Testing*, 64 MGT. SCI. 4471 (2018).

- **Financial markets**
  - On the firm side, Hertzberg, et al.,[127] and Doblas-Madrid and Minetti,[128] study the effects of information sharing on firms in credit markets. Doblas-Madrid and Minetti use contract-level data from a U.S. credit bureau in the equipment financing industry to examine the impact of lenders' access to information about borrowing firms' repayment performance on the credit performance of firms. They find that access to such information in their sample can reduce contract delinquencies and defaults, without loosening lending standards. Hertzberg, et al., using data from the Argentine public credit registry, further suggest that information sharing among lenders about borrowing firms' repayment performance may reduce the incidence of delinquencies and defaults, but that lenders may also reduce credit to a firm in anticipation of other lenders' reaction to negative news about the firm.
  - On the consumer side, Kim and Wagman[129] study the impact of opt-in and opt-out defaults that determine whether lenders can share information about borrowing consumers on certain aspects of mortgage markets. Using variation in the adoption of local financial-privacy ordinances in five California Bay Area counties, they suggest that more stringent restrictions on the sharing of consumer financial information[130] may reduce price competition. They argue that such a reduction may take place due to sellers' inability to offset potential downstream costs from loan defaults with revenues from monetizing information obtained in the application process, and, consequently, lenders' incentives to screen applications from consumers may weaken, contributing to higher rates of loan defaults.

---

[127] Andrew Hertzberg, et al., *Public Information and Coordination: Evidence from a Credit Registry Expansion*, 66 J. FIN. 379 (2011).
[128] Antonio Doblas-Madrid & Raoul Minetti, *Sharing Information in the Credit Market: Contract-level Evidence from U.S. Firms*, 109 J. FIN. ECON. 198 (2013).
[129] Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis*, 46 RAND J. ECON. 1 (2015).
[130] Specifically, in 2002, three out of five counties in the San Francisco-Oakland-Fremont, California Metropolitan Statistical Area adopted local ordinances that were more protective than previous practices, in that the new ordinances required financial institutions to seek written waivers from consumers before sharing information about those consumers with either affiliates or non-affiliates.

The above studies suggest that at least some degree of data sharing may be beneficial in lending or credit markets. Although the analyses in these studies focus specifically on financial transactions, their insights suggest that even in information categories that tend to be more sensitive, such as financial information, data sharing may be valuable from the perspectives of both consumer surplus and economic efficiency.

- **Online advertising:**

As a background matter, research suggests that consumer-related information is a key input into online advertising, valuable to both content providers and – at least (but not only) via ad-supported content – to consumers.[131] Correspondingly, "limiting online advertising's access to data about audience interests and demographics substantially reduces revenue to online content providers, by 50 to 70 percent."[132] Such limitations can also harm competition, and may have an outsize effect on small publishers.[133]

In addition, while there are various means of funding content, research regarding the value of ad-supported online content is a baseline consideration for questions about the potential impact of regulatory restrictions on the collection or use of data driving ad-supported content.

---

[131] For an overview of the literature, see J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, SSRN Working Paper 4279947 (Nov. 2022), https://ssrn.com/abstract=4279947 or http://dx.doi.org/10.2139/ssrn.4279947; *see also* Howard Beales & Jeffrey A. Eisenach, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content*, Navigant Econ. Technical Report (2014), https://digitaladvertisingalliance.org/sites/aboutads/files/files/DAA_images/fullvalueinfostudy%20-%20Navigant.pdf (finding a 66% drop in value without cookies.); Rene Laub, Klaus Miller, & Bernd Skiera, *The Economic Value of User Tracking for Publishers*, SSRN Working Paper 4251233 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4251233. Regarding consumer value and content, see, e.g., Hunt Allcott, Luca Braghieri, Sarah Eichmeyer & Matthew Gentzkow, *The Welfare Effects of Social Media,* 110 AM. ECON. REV. 629 (2020), 76.DOI: 10.1257/aer.2019065.

[132] Beales & Stivers, *supra* note 125 at ii.

[133] *Id.* (citing UK Digital Advertising Marketing Study).

- Alcott, et al., used a randomized large-n study of Facebook users to evaluate the consumer welfare effects of social media.[134] They examined the willingness to accept (WTA) of a sample of users to deactivate their Facebook accounts for four weeks, finding a median and mean WTA of $100 and $180 per user per four weeks, respectively. The WTA estimate means that "[a]ggregated across an estimated 172 million US Facebook users, the mean valuation implies that four weeks of Facebook generates $31 billion in consumer surplus in the US alone." Using diverse measures of consumer effects post-experiment, they found complex and somewhat mixed tradeoffs.
- Corrigan, et al., conducted a series of three non-hypothetical auction experiments where winners were paid to deactivate their Facebook accounts for a full year.[135] Though the subject populations were varied across the three experiments, the suggested WTAs were consistent: the average Facebook user would require more than $1,000 to deactivate their accounts for a year.
- Brynjolfsson, Collis, and Eggers use a combination of different survey methodologies to show that high levels of consumer surplus are associated with free online content.[136] Using willingness-to-accept estimates, they found that the median 2016 consumer valued online search at $14,760 per year, while valuing the rest of the Internet at $10,937 per year, or roughly $8.3 trillion in aggregate for the U.S.
- In a 2018 Federal Reserve Bank of Philadelphia Working paper, Nakamura, et al. analyzed the contribution of "free" content to domestic production based on the cost of production; they estimated that such content added $294 billion to U.S. GDP.[137]

---

[134] Hunt Allcott, Luca Braghieri, Sarah Eichmeyer & Matthew Gentzkow, *The Welfare Effects of Social Media,* 110 AM. ECON. REV. 629 (2020), 76.DOI: 10.1257/aer.2019065

[135] Jay R. Corrigan, *et al.*, H*ow Much Is Social Media Worth? Estimating the Value of Facebook by Paying Users to Stop Using It*, PLOS ONE (2018). https://doi.org/10.1371/journal.pone.0207101.

[136] Erik Brynjolfsson, Avinash Collis & Felix Eggers, *Using Massive Online Choice Experiments to Measure Changes in Well-being*, 15 PROC. NAT'L ACAD. SCI.7520 (2019).

[137] Leonard Nakamura, et al., *"Free" Internet Content: Web 1.0, Web 2.0, and the Sources of Economic Growth*, Fed. Reserve Bank of Philadelphia Working Papers, WP 18-17 (2018), https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2018/wp18-17.pdf.

Other studies have sought to estimate the impact of privacy policies – both regulatory and private policies – directly.

- In "Privacy Regulation and Online Advertising," Goldfarb and Tucker examine the effects of the implementation of the 2002 European Union (EU) ePrivacy Directive, which preceded the GDPR.[138] The 2002 directive limited the ability of advertising networks to collect user data to facilitate the targeting of ads, and conclude that, after it took effect, advertising effectiveness in the EU in their sample decreased significantly. Their study used the responses of 3.3 million survey-takers who had been randomly exposed to 9,596 online banner ad campaigns. For each of the 9,596 campaigns, their dataset contains a treatment group exposed to the ads and a control group exposed to a public service ad. To measure ad effectiveness, they use a short survey conducted with both groups of users about their purchase intent towards an advertised product. They find that, following the ePrivacy Directive, banner ads in their sample experienced a reduction in effectiveness of over 65%, with no similar changes in non-European countries during a similar timeframe. They assert that it is possible that data rights can have a detrimental effect on the efficiency of online advertising.
- A study by Johnson, Shriver, and Du[139] examines the AdChoices Program, an ad industry program (begun in the U.S.) that enables consumers to opt out of behavioral advertising via a dedicated website that can be reached by clicking an AdChoices icon overlaid on internet ads.[140] Based on a data sample from an ad exchange, they find evidence that suggests that US users who opt out fetch 52% less ad revenue on the exchange than users who allow behavioral targeting, who are presented with comparable ads. They assert that these costs are borne by publishers and by the exchange, and they observe similar results in their sample for the EU and Canada. A related study by Goldberg, Johnson, and Shriver, using a data

[138] Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGT. SCI. 57 (2011).
[139] Garrett Johnson, Scott Shriver & Shaoyin Du, *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?*, 39 MRK. SCI. 33 (2020).
[140] *Id.*

sample from Adobe's website analytics platform, finds reductions in EU user website traffic and revenue after the implementation date of the GDPR, and demonstrates evidence suggesting that at least some of these reductions were due to the regulation.[141]

- Peukert, et al. examined short-run changes in web sites and the web tech industry by examining over 110,000 web sites and their third-party HTTP requests for twelve months prior to, and six months following, GDPR's 2018 effective date.[142] They found that all firms suffered losses associated with GDPR. In addition, they found an increase in market concentration, with Google, the largest vendor, suffering relatively smaller losses while increasing its market share in advertising and analytics. They also found evidence suggesting that the usage of third-party web cookies has declined in recent years, in part due to private-sector initiatives such as Intelligent Tracking Prevention (ITP), as well as legislations, such as the GDPR.
- Beales and Eisenach examine the value of information sharing in online advertising by analyzing two data sets.[143] First, based on a large, impression-level database of advertising placements provided by two anonymous firms that operate advertising exchanges with automated bidding, they estimate that cookies increase advertisers' willingness to pay by at least 60 percent (for users with recent cookies), and by as much as 200 percent (for users with longer-lived cookies).[144] Their results also suggest that, all else equal, cookies confer greater value to smaller publishers. Based on observations of display ad placements for the top 4000 publisher, they find that third-party advertising tech models account for roughly half of advertising activity among top-ranked websites,

---

[141] These empirical findings are further supported by theoretical work. For instance, Sharma et al. (2021, https://ssrn.com/abstract=3503065) generate predictions from a theoretical framework of competing ad networks and heterogeneous publishers, with equilibrium dynamics that predict reductions in ad revenues for publishers and ad networks, and larger percentages reductions for smaller publishers and ad networks.
[142] Christian Peukert et al., *Regulatory Spillovers and Data Governance: Evidence from the GDPR*, 41 MKTG. SCI. 318 (2022).
[143] J. Howard Beales & Jeffrey A. Eisenach, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content*, Navigant Econ. Technical Report (2014), https://digitaladvertisingalliance.org/sites/aboutads/files/files/DAA_images/fullvalueinfostudy%20-%20Navigant.pdf.
[144] *Id.* at 11-12.

and roughly two-thirds of advertising activity among websites in lower cohorts.[145] Their findings also indicate that long-tail websites are disproportionately dependent on ad intermediaries.[146]

- Laub, Miller, and Skiera examine 42 million ad impressions from 100 publishers and find a 60 percent decrease in the raw mean net price paid to publishers for ad impressions without user tracking, and a 14 percent decrease after controlling for differences in users, advertisers, and publishers behind those ad impressions.[147] In addition, they find that more than 70 percent of publishers realize lower net prices when user tracking is unavailable, and that publishers providing broad content, such as news sites, suffer more from consumer tracking restrictions than publishers with more focused content.
- Other researchers have questioned the extent to which web publishers may benefit from targeted advertising; for example, a study of a certain media company's numerous sites by Marotta, et al., suggests that web publishers derive a 4% increase in revenue from engaging in targeted advertising.[148] That is, of course, a positive increase in revenue, but a considerably smaller one than that suggested by other studies. One might question the extent to which a single media firm's sites are representative, but perhaps the broader takeaway is that the magnitude of the GDPR's effect is not evenly distributed across firms.
- Ad exchanges may be able to offset some of the reductions in data from a subset of users. For example, a study by Aridor, Che, and Salz,[149] based on a sample from an ad intermediary in the travel industry, suggests that the intermediary they studied was able to use predictive analytics to make up for its data shortfall from approximately 12.5% of

---

[145] *Id.* at 16.
[146] *Id.*
[147] Rene Laub, Klaus Miller, & Bernd Skiera, *The Economic Value of User Tracking for Publishers*, SSRN Working Paper 4251233 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4251233.
[148] Veronica Marotta, et al., *Online Tracking and Publishers' Revenues: An Empirical Analysis*, Workshop of Information Systems Economics (WISE) (2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.
[149] Guy Aridor, Yeon-Koo Che, & Tobias Salz, The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR (NBER Working Paper No. 26900, 2020). https://www.nber.org/papers/w26900.pdf.

users who chose not to be tracked after GDPR; moreover, the intermediary was able to better track data and monetize ads from those users who chose to be tracked.

- A new working paper by Johnson, et al. (2023)[150] examines the effect of a regulatory enforcement action; that is, YouTube's 2019 settlement of FTC allegations that YouTube had violated the COPPA Privacy Rule, which implements the Children's Online Privacy Protection Act (COPPA).[151] Under that Consent Decree, YouTube agreed to remove all forms of personalization – including personalized advertising, personalized search, and content recommendations – for "child-directed" content, beginning in January 2020. Examining the impact on 5,066 top American YouTube channels, the study found that,

  > Consistent with a loss in personalized ad revenue, we find that child-directed content creators produce 13% less content and pivot towards producing non-child-directed content. On the demand side, views of child-directed channels fall by 22%. Consistent with the platform's degraded capacity to match viewers to content, we find that content creation and content views become more concentrated among top child-directed YouTube channels.[152]

  Whether the results implicate a total welfare loss (or a total consumer welfare loss) may be unclear, but the supply-side and demand-side observations are striking, as is the competitive impact favoring the top child-directed YouTube channels.
- Regarding firms' posted policies – as opposed to regulation – Strahilevitz and Kugler conducted an experiment employing excerpts from privacy policies from Facebook, Google, and Yahoo, along with fictional policy excerpts drafted by the researchers.[153]

---

[150] Garrett Johnson, Tesary Lin, James C. Cooper & Liang Zhong, *COPPAcalypse? The YouTube Settlement's Impact on Kids Content* (April 26, 2023),
SSRN: https://ssrn.com/abstract=4430334 or http://dx.doi.org/10.2139/ssrn.4430334.

[151] Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, Sept. 4, 2019, https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law.

[152] *Id.*

[153] Strahilevitz & Kugler, *supra* note 110.

> They found that many subjects read the policies closely and understood them,[154] but that only about one third of the subjects indicated any willingness to pay any amount of money at all for access to email services that would not employ content-based analysis of the users' emails to serve personalized advertising. Of those who were willing to pay, median WTP was only $15 per year.

While the precise effects may be difficult to measure,[155] and may vary across publishers and exchanges, the impact of potential or actual losses in advertising revenue may merit consideration of potential downstream effects on competition and consumer surplus. The above studies strongly suggest some potential tradeoffs between a strengthening of data protections and the ability of firms to generate revenues through targeted ads and other data-reliant means. Still, they leave a number of questions unanswered. For example, do targeted ads benefit or harm consumers on net, both individually and in aggregate. Also, to what extent may firms may develop other means of segmenting consumers, and to what extent might such tools function as close substitutes? We might also ask about spillover effects – for example, how consumers' choices to share (or not share) certain information with firms may affect (or be affected by) the choices made by and the experiences of other consumer segments.[156]

- **New firms and investment**

The connection between data rights and new firm formation is highlighted by recent research on the impact of the EU's 2018 General Data Protection Regulation (GDPR) on investment in new technology ventures.

---

154 This finding is somewhat at odds with the research regarding policy readability cited in note 110, *supra*.

155 Regarding some of the difficulties associated with measuring the causal effects of digital advertising, see, e.g., Brett Gordon, et al., *A Comparison of Approaches to Advertising Measurement: Evidence from Big Field Experiments at Facebook*, 38 MARKETING SCI. 193 (2019).

156 A study by Goh, Hui and Png, for instance, identifies empirical evidence suggesting that the ability to opt out — in their case, of spam calls via the U.S. Do Not Call Registry — may result in an increase in the volume of calls to those consumers who do not opt out. O'Brien and Smith, 2014, offer a theoretical analysis of other potential spillovers that may occur when consumers choose (not) to share information with firms.

- Jia, Jin, and Wagman analyze venture investment data from two databases that track global venture investments and find evidence suggesting dramatic drops in investments in newer, 0-6 year old EU technology ventures after GDPR.[157] Their findings hold more strongly for consumer-facing ventures that are in their initial development stages,[158] as well as for financing transactions led by foreign investors.[159] The authors find evidence suggesting that the effects on EU technology ventures persist at least 2.5 years after the GDPR's implementation date in May 2018, although they also find that the effects somewhat weaken over time.[160] While further, and broader, study of the impact of GDPR is warranted, the magnitude and persistence of the effects on venture capital investment in their early findings suggest the potential for substantial effects, at least for certain data rights. It will be important to see what such effects look like over the longer run, as businesses and regulators adjust to the effects of the regulation.

- **Telecomm**

  - Adjerid & de Matos studied a series of field experiments launched by a large telecom provider after GDPR.[161] The field experiments had been designed to foster user consent, as required under GDPR, and the study indicated that the field tests were highly successful. As a result, the telecom provider was able to process more personal data after GDPR than it was before. To the extent this finding can be

[157] Jian Jia, Ginger Zhe Jin & Liad Wagman, *The Short-Run Effects of GDPR on Technology Venture Investment*, MRK. SCI. 661 (2021).
[158] *Id.*
[159] Jian Jia, Ginger Zhe Jin, & Liad Wagman, *Data Regulation and Technology Venture Investment: What Do We Learn from GDPR?*, CPI ANTITRUST CHRONICLE (2021).
[160] Jian Jia, Ginger Zhe Jin, & Liad Wagman, *The Persisting Effects of the EU General Data Protection Regulation on Technology Venture Investment*, ANTITRUST SOURCE, June 2021.
[161] Idris Adjerid & Miguel Godinho de Matos, *Consumer Behavior and Firm Targeting after GDPR: The Case of a Telecom Provider in Europe*, 68 MGMT. SCI. 3330 (2019).

generalized, it may suggest that large well-resourced firms are better able to minimize the impact of GDPR (and similar regulations) on consumer access.

The Competitive Effects of Privacy Regulation

The aforementioned studies suggest that the effects of the GDPR — an omnibus data protection regulation — may have been, at least in the short term, especially pronounced for nascent EU technology ventures. In addition, they suggest that large well-resourced firms have been better able to minimize the impact of GDPR. Labeling certain restrictions fundamental rights seems a clear way of assigning some importance to them, but it is largely unhelpful from an economic or analytic standpoint. Neither nominated rights – such as "the right to be forgotten" – nor their specific implementation in GDPR seem derived from any principles that would help order rights or interests, or approach tradeoffs between them in any systematic way. Still, it remains unclear which specific components of the GDPR may have led to observed effects, and whether those provisions would have the same impact in other jurisdictions. The observed effects are significant, and in our view, policy makers going forward ought not to ignore them, keeping in mind that the literature is developing, and that available studies do not answer the question whether the GDPR's effects on products and services that are (or that may have been) provided by those nascent ventures resulted in a net gain or loss for consumer surplus and economic efficiency.

Several of the research summaries above – organized roughly by sector – directly implicate competitive effects. To recap,

- Kim and Wagman's findings suggest that more stringent restrictions on the sharing of consumer financial information may reduce price competition.[162]
- Jia, Jin, and Wagman found dramatic drops in investments in newer, 0 – 6 year-old EU technology ventures after GDPR,[163] and that their findings were stronger for consumer-

[162] Kim and Wagman, *supra* note 123.
[163] Jia, Jin & Wagman, *supra* note 151.

facing ventures in their initial development stages,[164] and for financing transactions led by foreign investors.[165]

- Johnson, Shriver, and Du found, among other things, that opt-out standards may be borne by publishers, and by ad exchanges.[166]
- Laub, Miller, and Skiera found that lower net prices associated with a loss of user tracking was disproportionately great for publishers providing broad content, such as news sites, suffer more from consumer tracking restrictions than publishers with more focused content.[167]
- Beales and Eisenach suggested that cookies confer greater value to smaller publishers, and that long-tail websites are disproportionately dependent on ad intermediaries.[168]
- Peukert, et al., found an increase in market concentration associated with GDPR;[169] they also found that, while all firms suffered losses associated with GDPR, Google, the largest vendor, suffered relatively smaller losses while increasing its market share in advertising and analytics.
- Adjerid & de Matos[170] may suggest that large well-resourced firms are better able to minimize the impact of GDPR (and similar regulations) on consumer access, in addition to the general incumbency advantages described by Campbell, *et al.*
- Johnson, et al. (2023), observed that content creation and content views became more concentrated among top child-directed YouTube channels because of the settlement of a specific COPPA enforcement action in 2019.[171] Johnson provides a useful review of research on the impact of GDPR,[172] summarizing that "The GDPR hurt firm

---

[164] *Id.*

[165] Jian Jia, Ginger Zhe Jin, & Liad Wagman, *Data Regulation and Technology Venture Investment: What Do We Learn from GDPR?*, CPI ANTITRUST CHRONICLE (2021).

[166] Johnson, Shriver & Du, *supra* note 133; *see also* Beales & Stivers,

[167] Laub, Miller & Skiera, *supra* note 141

[168] Beales & Eisenach, *supra* note 137.

[169] Peukert, et al., *supra* note 136.

[170] Adjerid & de Matos, *supra* note 155

[171] *See* notes 144-146, *supra*.

[172] *See* Johnson, *Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond*, *supra* note 93, *supra*.

> performance by imposing costs, decreasing revenue, and thereby hurting profitability. Venture funding for technology firms fell—particularly for more data-related ventures. The GDPR limited economic dynamism by accelerating market exit and slowing entry. … [T]he GDPR hurt competition by creating greater harms for smaller firms and by increasing market concentration in the data vendor market."[173]

As a general matter, regulations that impose substantial fixed costs on affected firms tend to burden smaller firms and entrants more than they do large firms and incumbents.[174] As Catherine Tucker & Alex Marthews explain in a Brookings Economics Report:

> From an economics perspective, when modeling the effects of privacy regulation on the ability of firms to compete, one starting point is the observation that in theory, any regulation that imposes any fixed costs on firms will have an anti-competitive effect. . . .The concern is that if compliance has a fixed cost, then that fixed cost will be more heavily felt by a smaller firm with smaller revenues, putting smaller firms at a cost disadvantage relative to larger firms, or at least only weakly increasing in firm size.[175]

Incumbents' relative advantages might skew further, to the extent that, e.g., "in-house" regulatory expertise can lower the cost of compliance for privacy and data security regulations. Moreover, even good-faith and productive contributions of incumbents to the rulemaking process, standard setting, and related activities may further tilt the field. To the extent that costly compliance practices reflect firm policies, they may be not merely fixed costs but – at least some incumbents and to some extent – both fixed and sunk. To be clear, such anticompetitive effects do not necessarily imply that the regulations are

---

[173] *Id.* at 3.
[174] *See, e.g.*, Caleb S. Fuller, *The Perils of Privacy Regulation*, 30 REV. AUSTRIAN ECON. 30193 (2017).
[175] Alex Marthews & Catherine Tucker, *Privacy Policy and Competition*, ECON. STUD. AT BROOKINGS 8 (2019), https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf.

anticompetitive on net; rather, they suggest that certain competitive costs may be associated with such regulations.

- Campbell, Goldfarb, and Tucker model the frictions imposed by consent requirements, and demonstrate that privacy regimes that include a consent requirement can further exacerbate incumbents' advantages.[176] In brief, the likelihood of consumer consent will vary according to, among other factors, (a) the longevity of a consumer's relationship with a given firm and (b) the scope of benefits consumers expect to receive from the firm (and, hence, from the grant of consent). These will tend to favor established firms (incumbents) and firms offering a broader array of products or services, even where a smaller "niche" firm offers a higher quality product or service.[177] They show that "privacy regulation can preclude profitable entry by the specialist firm," and that the impact of these types of regulations are "strongest in industries with little price flexibility," which may be especially important for ad-supported or other zero-price Internet products.[178] They also show that their results are robust to several specialist firms serving different niches. And allowing for investment in quality, their model shows that the entrant never invests more in quality under regulation than without regulation, and in some cases invests less.
- Using data from PrivacyGrade.org—which provides a privacy grade or rating for each app in the Android app marketplace, along with metrics for app quality and usage—Cooper & Yun find "no relationship... between privacy grades and our proxies for market power—market shares... and market concentration."[179] They also find "a negative relationship between privacy levels and quality ratings, suggesting a tradeoff between privacy and other dimensions of product quality that consumers

[176] James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47 (2015).
[177] *Id.* At 48.
[178] *Id.*
[179] James C. Cooper & John M. Yun, *Antitrust and Privacy: It's Complicated*, Vol. 2022 U. ILL. J.L. TECH. & POL'Y 343, 348 (2022)

value."[180] Analysis of alternative web-traffic data and a competing source of privacy ratings also fails to find a relationship between privacy ratings and market shares or concentration.[181]

- Adjerid & de Matos studied a series of field experiments launched by a large telecom provider after GDPR.[182] The field experiments had been designed to foster user consent, as required under GDPR, and the study indicated that the field tests were highly successful. As a result, the telecom provider was able to process more personal data after GDPR than it was before. To the extent this finding can be generalized, it may suggest that large well-resourced firms are better able to minimize the impact of GDPR (and similar regulations) on consumer access.
- Janßen, *et al.*, surveyed 4.1 million apps on the Google Play store between 2016 and 2019 and observed that "GDPR sharply curtailed the number of available apps."[183] In particular. "GDPR precipitated the exit of over a third of available apps; and following its enactment, the rate of new entry fell by 47.2 percent, in effect creating a lost generation of apps."[184]

III. Economics and Privacy Regulation

a. Guiding Principles

In market environments with asymmetric information, the ability to sort parties into different types (e.g., high and low productivity workers, high and low value users, high and low quality sellers) can enhance efficiency by allowing better matching of action (e.g., price, wage, advertisement, product recommendation, purchase decision) with type.[185] However, even in cases where markets function better with more information (e.g., better

---

[180] *Id.*

[181] *Id.* (examining website-traffic data from SimilarWeb and privacy ratings from DuckDuckGo for sites in 37 categories).

[182] Idris Adjerid & Miguel Godinho de Matos, *Consumer Behavior and Firm Targeting after GDPR: The Case of a Telecom Provider in Europe*, 68 MGMT. SCI. 3330 (2019).

[183] Janßen, *et al.*, *GDPR and the Lost Generation of Innovative Apps*, NBER Working Paper Series (2022) at 2, *available at* https://www.nber.org/system/files/working_papers/w30028/w30028.pdf.

[184] *Id.*

[185] *See, e.g.*, Stigler, *supra* note 65 (regarding workers and credit seekers, among others); James C. Cooper, *Separation Anxiety*, 21 VA. J. L. & TECH. 1 (2017) (regarding pooling and separation generally).

matching of buyers with sellers), privacy may provide important countervailing benefits. Identifying and measuring such benefits may require further inquiry, but policy makers, regulators and researchers should be attuned to potential tradeoffs for several reasons.

First, individuals may desire to keep certain aspects of their lives private due to, among other considerations, a desire to maintain a sense of personal dignity, security and safety concerns, and financial reasons. Second, such concerns, and a perception of poor or uncertain privacy protection, can diminish consumer trust and chill beneficial behavior. Recognition of this fact in abstract, if not as measured, lies behind legal duties of confidentiality between doctors and patients and lawyers and their clients—requiring a recipient of information to refrain from sharing it can foster the beneficial sharing of information. For example, there is evidence that symptomatic patients may be more inclined to share useful information, and respond to practitioners' questions honestly and fully, if the patients trust that the information they divulge will be maintained in confidence;[186] they may also be more likely to present themselves to health care providers in the first place.[187] Further, a perceived lack of privacy, or of the risk of privacy violations, can chill consumers from providing and acquiring information about sensitive topics for fear of social approbation. For instance, individuals who feel unwell may hesitate to search for potentially helpful information on a search engine or to acquire remedies from sellers.[188]

Moreover, many policies—however well-conceived and implemented—entail costs as well as benefits. With privacy policy specifically, it is important to emphasize that the

---

[186] *See, e.g.*, Celeste Campos-Castillo & Denise L. Anthony, *The Double-edged Sword of Electronic Health Records: Implications for Patient Disclosure*, 22 J. AM. MED. INFORM. ASS'N e130 (2015); Israel T. Agaku, et al., *Concern about Security and Privacy, and Perceived Control over the Collection and Use of Health Information are Related to Withholding of Health Information from Healthcare Providers*, 21 J. AM. MED. INFORM. ASS'N 374 (2014).

[187] *See, e.g.*, Kenneth R. Ginsburg, et al., *Adolescents' Perceptions of Factors Affecting Their Decisions to Seek Health Care*, 273 JAMA 1913 (1995).

[188] *See generally* Benjamin Wittes & Jodie C. Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, Ctr. for Tech. Innovation at Brookings (2015), https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf; Ginger Zhe Jin & Andrew Stivers, *Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics*, SSRN Working Paper (May 22, 2017), https://ssrn.com/abstract=3006172 or http://dx.doi.org/10.2139/ssrn.3006172., Alex Marthews & Catherine Tucker, *Impacts of Surveillance on Behavior*, in CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 437 (David C. Gray & Stephen Henderson eds., 2017); Cooper, *supra* note 177.

benefits of a privacy policy that applies uniformly across all consumers, or across a given domain, industry, or type of conduct, may be heterogeneous, ambiguous, uncertain, or unstable. A privacy policy (or policy change) may benefit some consumers but not others, and it may do so to a greater or lesser extent than alternative policies. For example, price differentiation based on consumer information may raise prices for some consumers while lowering prices for others.[189] Similarly, harm due to worse terms that arise from better matching (of buyers and sellers or consumers and products, for example), may or may not be harmful to all consumers or to aggregate consumer welfare.[190] For instance, although certain consumers may receive worse terms when their types are revealed (e.g., low-productivity worker, high-valuation consumer, higher credit risk individual) than they would when pooled together (where all consumers are treated as an "average consumer"), other consumers may enjoy better terms, and aggregate consumer welfare may increase. Further, if separation among different consumer "types" is coupled with drawing more consumers into the market (e.g., by availing discounts to consumers who have lower willingness to pay) or by reducing costs (e.g., the costs of matching products with consumers, for instance, in insurance and lending markets), such separation may also increase aggregate welfare by expanding market accessibility and increasing output.[191]

---

[189] *See*, for instance, Taylor and Wagman, *supra* note 67, where it is shown that under a simple setting of price discriminating sellers, different privacy policies with respect to consumers' preferences can benefit some consumers while harming others.

[190] Some matching can lead to separation on dimensions that society has deemed harmful, independent of the question whether the harms are – or are deemed – privacy harms *per se*. For example, due to their discriminatory impact (e.g., race, religion, gender, or sexual orientation). In addition, even matching that society has not necessarily deemed harmful – for instance, the use of information to target vulnerable populations who are more likely to fall for fraudulent or deceptive product offerings (e.g., "sucker lists") – can be dissipative, as this type of matching, when there are no externalities, may constitute a transfer of wealth from a gullible consumer to a potential fraudster; when there are negative externalities, such matching can reduce total welfare. To the extent that these types of segmentation are discriminatory or lead to deception, they can be addressed under anti-discrimination laws or under the FTC's deception or unfairness authority. At the same time, some matching predictions may lead to inaccuracies that result in denial of opportunities to a subset of consumers (e.g., credit or employment). Because firms have incentives to correctly classify consumers, it is uncertain that regulatory intervention can improve market incentives. Further, with respect to credit, the Fair Credit Reporting Act provides consumers with broad inspection and correction rights.

[191] *See, e.g.*, Cooper, *supra* note 177; Burke, et al., supra note 65; Kim & Wagman, *supra* note 123. Caveats may exist if consumers may seek to avoid such separation by expending efforts. *See, e.g.*, Vincent Conitzer, et al., *Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases*, 31 MKTG. SCI. 277 (2012).

b. Enforcement Goals

Privacy and competition are distinct policy goals. While they may both be implicated in any individual policy proposal or decision, they are distinct objectives and are often protected by different rules and enforcement functions.[192] At the same time, assigning or establishing data protections can have complex competitive effects. Such protections may create presumptions or defaults about who owns, and has the right to exclude others from using, valuable information. This assignment to one party or another may clarify the terms under which marketplace actors can transact and transfer data, potentially reducing ambiguity or other uncertainty about the locus or scope of data rights. At the same time, the creation, assignment, and specific implementation of privacy protections can have complex effects, which, on net, may or may not be efficiency enhancing.

Among other objectives, a primary goal of an enforcement regime is to deter prohibited (harmful or otherwise undesirable) conduct. In so doing, enforcement should at least mitigate consumer harms that are not adequately mitigated or compensated by other available remedies. Often, the focus is on consumer harm that is not (adequately) mediated or ameliorated through the market, perhaps due to systematic and durable market failure. In the context of privacy, for instance, an enforcement regime might focus on harmful commercial data practices of which consumers are unaware and with regard to which, for that reason or others, they cannot bargain. For example, firms may have considerable private information regarding their own privacy and data security practices, and about the extent to which those practices align (or fail to align) with their advertising and/or marketing of those practices; and numerous FTC enforcement matters under Section 5 of the FTC Act are based on false or misleading material statements, or material omissions, about such firm conduct.[193]

---

[192] For a general discussion, see, e.g., Ohlhausen & Okuliar, *supra* note 16.

[193] *See, e.g.*, Facebook, Inc., Fed. Trade Comm'n Docket No. C-4365 (2012) (admin. complaint). In numerous cases, false or misleading claims about compliance with the EU-U.S. Privacy Shield has been the basis for enforcement under Section 5 of the FTC Act. For example, in separate actions settled in 2020, the FTC alleged that five firms—DCR Workforce, Inc., Thru, Inc., LotaData, Inc., 214 Technologies, Inc., and Empiristat, Inc.—all falsely claimed in statements on their websites that they were certified under the EU-U.S. Privacy Shield framework, and that LotaData also falsely claimed that it was a certified participant in the Swiss-U.S. Privacy

In other cases, firm conduct may be deemed unfair, or both deceptive and unfair.[194] In another matter resolved by a consent order, it was alleged that the defendant, DesignerWare, had engaged in unfair practices when it installed monitoring and geolocation software on rented computers, gathered sensitive personal, financial, medical, and geophysical location information about consumers from those computers, and disclosed that personal information to rent-to-own store licensees, causing consumers harm and enabling rent-to-own store licensees with the means to cause consumers harm.[195] Consumers were unable to (reasonably) avoid those harms because the software was invisible to them, as were DesignerWare's disclosure practices. And in Retina-X Studios,[196] the FTC alleged that the developer of three "stalking apps"—which allowed purchasers to monitor the devices on which they were installed, without the device users' knowledge or permission—had violated both the deception and unfairness prongs of Section 5 of the FTC Act, in addition to violating the Children's Online Privacy Protection Act[197] (COPPA) by knowingly collecting personal information from children under the age of 13 through one of its stalking apps.

Broadly, there are two approaches to optimal deterrence of harmful conduct, though both approaches depend on the ability to identify such conduct with sufficient accuracy. First, an enforcement authority can assign liability for outcomes that are caused by firm conduct and set fines or penalties proportional to consumer harm in order to deter conduct

---

Shield framework, which establishes a data transfer process similar to the EU-U.S. Privacy Shield framework. Fed. Trade Comm'n, FTC Finalizes Settlements with Five Companies Related to Privacy Shield Allegations (2020), https://www.ftc.gov/news-events/press-releases/2020/01/ftc-finalizes-settlements-five-companies-related-privacy-shield (settlements with DCR Workforce, Inc., Thru, Inc., LotaData, Inc., 214, Inc., and EmpiriStat, Inc.); and in *Ortho-Clinical Diagnostics*, a provider of medical diagnostic devices and services agreed to settle FTC allegations that the firm had misled consumers about its handling of personal data and its purported compliance with the EU-US Privacy Shield framework. Ortho-Clinical Diagnostics, Inc., FTC File No. 192 3050 (2020) (decision and order), https://www.ftc.gov/enforcement/cases-proceedings/192-3050/ortho-clinical-diagnostics-inc-matter,

[194] Links to FTC consumer privacy and data security matters, including those regarding deceptive practices, unfair practices, or practices that are both unfair and deceptive may be found at https://www.ftc.gov/enforcement/cases-proceedings/terms/245%2B247%2B249%2B262.

[195] In the Matter of DesignerWare, LLC, FTC Docket No. C-4390 (2013), https://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter.

[196] Retina-X Studios, LLC, FTC Docket No. C-4711 (2020) (decision and order).

[197] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505; implementing regulations enforced by the FTC are at 16 CFR Part 312.

that creates net social harm.[198] With harm-based penalties, firms are forced to internalize the harm their actions cause, giving rise to incentives to take greater precautions to avoid harm and engage in lower levels of harmful activity. In *Wyndham*,[199] for example, detection of demonstrable consumer harm—large clusters of fraudulent credit card usage—figured in the investigation of the firm's data security practices, and of its representations about those practices.

Published material from the FTC's Bureau of Economics outlines an approach to assessing consumer harm that could be applied to matters such as *Wyndham*, where the alleged harms included both direct financial losses and time spent to remedy those losses and guard against future ones.[200] The approach takes into account the estimated baseline rate of identity theft, conditional on a consumer's being subject to a breach. And, because the Section 5 violation was predicated on the firm's deceptive statements, FTC Bureau of Economics staff also estimated the price premium that consumers paid due to those deceptive statements, multiplied by an estimate of the number of consumers affected,[201] although the relief actually obtained in the matter was not monetary but behavioral, comprising a comprehensive information security program, annual information security audits, and other safeguards.[202]

A similar range of harms was observed in a larger data breach involving Equifax, the credit rating agency. That matter arose from a publicly disclosed data breach involving the

---

[198] Under the FTC Act, remedies may require the payment of damages. 15 U.S.C. 57b. More broadly, however, assessment of remedies may be harm based, but is not necessarily confined to damages. For example, Section 5(m) of the FTC Act stipulates various factors pertinent to determining the magnitude of monetary penalties for knowing violations; and under Section 19, a court may order "such relief as the court finds necessary to redress injury to consumers or other persons," including, but not limited to, payment of damages, refund or money or return of property, and the recission of contracts.

[199] FTC v. Wyndham Worldwide Corp. et al., Civil No. 13-1887 (D.N.J. Apr. 7, 2014) (opinion denying defendant's motion to dismiss); 799 F.3d 236 (3d Cir. 2015).

[200] Dan Hanner, Ginger Zhe Jin, Marc Luppino & Ted Rosenbaum, *Economics at the FTC: Horizontal Mergers and Data Security*, 49 REV. INDUS. ORG. 613 (2016) (section on estimating harm from data breaches with application to *Wyndham* at 627 – 630).

[201] *Id.*

[202] Compliance with required behavioral relief imposes costs on the firm which could, in principle, be proportional to consumer harm, although in practice calibration of such costs may be difficult and other factors may dominate the design of behavioral relief. As a practical matter, policing behavioral relief may often be much more costly for the enforcer than the collection of money damages or monetary penalties.

theft of sensitive personal information from more than 147 million consumers.[203] The Commission's complaint alleged consumer harms including, *inter alia*, "wasted time and money to secure personal accounts and consumer reports from future identity theft, the cost of obtaining additional credit monitoring products or security freezes, and a significantly increased risk of becoming victims of identity theft in the future."[204] The increased risk of identity theft, even if not specified with precision across consumers, may be deemed a present and substantial harm, partly due to its scale, and to average harms associated with large breaches of sensitive personal information, including financial information, and not least because the risk was material to affected consumers, many of whom undertook costly steps to mitigate that risk.

Further, while some types of proscribed conduct do not entail cognizable consumer benefits, others do; and harm-based penalties do not preclude firms from engaging in conduct that, while causing some degree of harm, is beneficial on net. A regime based on addressing completed or likely harm is akin to protecting consumer data with a liability rule. This approach can at times be potentially superior to one that accords consumers property rights over information about them for two primary reasons. First, it is unclear who owns the rights to jointly produced information, such as a "retweet" or a "like" on a webpage, or to consumer-sourced health information that is filtered through a provider's expertise and technology. Second, it is likely that a non-negligible portion of consumers would be willing to sell the entitlement to use their data in many circumstances, but research has shown that the value of an average individual's data is likely to be low.[205]

A second enforcement approach is to sanction net harmful conduct by targeting a category of conduct that is established as being net harmful (e.g., fraud), and setting a

---

[203] FTC v. Equifax, Inc., Case 1:19-mi-99999-UNA Document 2361, 5 (N.D. Ga. 2019) (complaint)

[204] *Id.* at 14.

[205] *See, e.g.*, Acemoglu, et al., *supra* note 52. For empirical evidence, see, e.g., Alastair R. Beresford, et al., *Unwillingness to Pay for Privacy: A Field Experiment*, 117 ECON. LETTERS 25 (2012); Sarah Spiekermann, et al., *E-privacy in 2nd Generation E-commerce: Privacy Preferences Versus Actual Behavior*, Proceedings of the 3rd ACM Conference on Electronic Commerce, Tampa, FL, 38–47(2001); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE Security & Privacy, January/February 2005, pp. 24-30. There is also evidence suggesting that privacy valuations are context sensitive. *See, e.g.*, Janice Y. Tsai, et al., The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, 22 Inf. Sys. Res. 254 (2011).

penalty or a way of calculating a penalty that is sufficient to deter the conduct, but that might or might not be a function of the magnitude of consumer harm caused by the conduct. Where conduct is plainly and uniformly harmful, an appropriate penalty may require a cessation of business. For example, with the revenge porn matter, EMP Media, the FTC and state enforcers together alleged that the firm's website, MyEx.com, was dedicated solely to revenge porn, violating federal and state law by posting intimate images of people, together with their personal information, such as the name, address, employer, email address, and social media account information, without consent.[206] Victims were subject to threats, harassment, and the loss of employment, and in numerous instances, the defendants allegedly charged victims fees from $499 to $2,800 to remove their images and information from the site.[207] The settlement with one defendant included monetary penalties, but also prohibited the posting of intimate images and personal information of others on a website without notice and consent, required the destruction of all such intimate images and personal information in his possession, and banned charging individuals fees for removing such content from a website.[208] Various types of fraud involving improper use of consumers' personal information also serve no legitimate commercial or competitive purpose.[209]

Note that under this approach, sanctions do not necessarily have to be related to consumer harm to generate deterrence as long as the agency can accurately identify, and firms fully understand, the types of proscribed conduct. Under these conditions, sanctions only have to be large enough so that a firm will never find it profitable to engage in the

---

[206] Fed. Trade Comm'n, FTC and Nevada Seek to Halt Revenge Porn Site (2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-nevada-seek-halt-revenge-porn-site; FTC v. Emp Media, Inc., 2018 U.S. Dist. LEXIS 16463 (D. Nev. 2018) (complaint for permanent injunction and other equitable relief, at 5-6).

[207] FTC v. Emp Media, Inc. (complaint for permanent injunction and other equitable relief, at 14-17).

[208] FTC v. Emp Media, Inc., (order granting motion for default judgment and final order for permanent injunction and other relief, at 4-6).

[209] In 2018, fraudulent imposter scams were the leading grounds for complaints submitted to the FTC's Consumer Sentinel Database. Fed. Trade Comm'n, Imposter Scams Top Complaints Made to FTC in 2018, (Feb. 28, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/imposter-scams-top-complaints-made-ftc-2018. For example, fraudsters falsely claimed to be working for the Internal Revenue Service, Social Security Administration, or other federal agency, seeking, under false pretenses, to induce consumers to reveal sensitive personal information, such as their social security numbers, in addition to money. These types of scams serve no legitimate commercial or competitive purpose.

proscribed conduct. To that end, remedies are bounded from below by the gain to the firm, and have no particular upper bound; anything greater than the gain from engaging in the conduct will be deterring.[210] Because the conduct identified is presumed to be net harmful to society, there is less concern about over-deterrence, provided there is sufficient clarity about the proscribed category of conduct and sufficient certainty (or a mechanism for establishing sufficient certainty) about whether a firm engaged in the proscribed conduct.[211]

More generally, a lower bound of remedies established by gains to the violating firm is consistent with an approach that requires the disgorgement of ill-gotten gains. And we note that, under the FTC Act, penalties may include "the refund of money or return of property," as well as damages and equitable relief such as the recision or reformation of contracts. [212] In *Vizio*, for example, the FTC obtained relief that included, but was not limited to, the disgorgement of ill-gotten monies.[213] In that matter, the Commission had alleged that the defendant engaged in both unfair and deceptive practices by surreptitiously recording and decoding consumers' TV viewing, and by selling consumers' viewing histories to advertisers and others, in some cases without any notice, and in others with representations that were not sufficiently clear or prominent to alert consumers to the firm's practices related to data collection and the sale of licenses.

c. Enforcement Approaches

U.S. privacy enforcement comprises a diverse collection of federal and state laws and regulations, in addition to private regulation via certain common law actions sounding in

---

[210] Louis Kaplow, *The Optimal Probability and Magnitude of Fines for Acts That Are Definitely Undesirable*, 12 INT'L REV. L. & ECON. 3 (1992).

[211] In the absence of sufficient certainty or a mechanism for establishing it, there is a probability that penalties will not be imposed. To the extent that firms are rational actors, they will incorporate the probabilities of enforcement into their decision-making, establishing a level of deterrence from engaging in the proscribed conduct as a function of the likely penalties and enforcement probabilities. If the expected costs to a firm, factoring in both the penalties and enforcement probabilities, are sufficiently high, the firm would be deterred from engaging in the proscribed conduct.

[212] 15 USC 57(b).

[213] FTC v. Vizio, Inc., Case 2:17-cv-00758 (D.N.J. 2017). The FTC brought the matter jointly with the State of New Jersey, and obtained both monetary and behavioral relief.

torts. All 50 states now have laws requiring notifications of data breaches (with variations in the speed, circumstances, penalties, and parties that have to be informed). Rather than being general or inter-sectoral, U.S privacy laws tend to be sector-specific, such as the privacy and data security regulations implementing parts of the Health Insurance Portability and Accountability Act (HIPAA), or issue-specific, such as the Children's Online Privacy Protection Act (COPPA) and its implementing rule, which is enforced by the FTC.

At the same time, there is a large body of privacy and data-security enforcement ranging across industry sectors, under Section 5 of the FTC Act.[214] The FTC Act does not specify or prohibit privacy violations per se, but it does prohibit, *inter alia*, "unfair or deceptive acts or practices in or affecting commerce."[215] Under that authority, the FTC has brought more than 200 cases alleging such prohibited conduct involving consumer privacy issues, and more than 60 involving data security issues; and the Commission has issued orders requiring diverse and substantial conduct remedies, and has imposed penalties as large as five billion dollars.[216] These efforts have forced organizations to examine what data they are collecting, for what uses, and how they manage, store, and share data.

Consumer harm may be more readily quantifiable when privacy invasions involve potential monetary losses. In other cases, when certain practices are shown or are known to cause net intangible privacy harm or are presumptively unfair or deceptive (e.g., surreptitious recording of intimate behavior in one's home), heightened penalties can facilitate deterrence.[217] For conduct that implicates intangible privacy harms but is not presumptively unfair or deceptive, economic frameworks may be used to argue that the conduct creates net harm.[218] Estimates need not be precise to order likely harms and benefits; and while a complete benefit-cost analysis may be infeasible for a specific case, countervailing benefits from, for instance, improved data flows in the specific market in

---

[214] 15 U.S.C. § 45.
[215] 15 U.S.C. § 45(a)(1).
[216] *See, e.g.*, Fed. Trade Comm'n, Privacy & Data Security: Update: 2019, https://www.ftc.gov/news-events/press-releases/2020/02/ftc-releases-2019-privacy-data-security-update.
[217] *See* text accompanying notes 199-203, *supra*.
[218] Regarding cost-benefit analyses in privacy policy, see, e.g., Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON L. REV. 1055 (2013).

question, may be taken into account; and in doing so, an enforcer might include the available empirical evidence that certain restrictions on data flows can have adverse effects on competition and consumers.[219]

The FTC's deception and unfairness authorities are consistent with the policy goals of promoting market efficiency and maximizing consumer welfare; and, as previously noted, FTC privacy-related enforcement actions incorporate elements of an economic approach to privacy where possible. First, as a practical matter, staff from the FTC's Bureau of Economics are typically assigned to privacy investigations, among others. Second, as a statutory matter, an act or practice that is "unfair" under Section 5 of the FTC Act must cause, or be 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."[220] With regard to deception, the Commission has clearly stated that "[c]ertain elements undergird all deception cases."[221] In particular, "the 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."[222] As with unfairness, consumer harm is a central element of liability, if it may be established less directly, through the requirement of materiality:

The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. If so, the practice is

---

[219] Under other circumstances, stipulated statutory or regulatory penalties, such as fines, may be efficient from a process and notice point of view. For example, where the harms to be deterred are varied in their particulars, and are small or frequent (or numerous), estimation of the harm may itself be relatively costly. Express statutory penalties under the FTC Act tend to be stipulated as alternatives, and not as fixed mandatory fines. For example, penalties under sections 5(i) and 5(m) of the FTC Act are to be "not more than $10,000 per violation," a figure that has been modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. §2461, amended by the Federal Civil Penalties Inflation Adjustment Improvements Act of 2015, Public Law 114-74, sec. 701, 129 Stat. 599 (2015), and Section 1.98(d) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(d), such that, e.g., monetary civil penalties a court may award under Section 5(m) are not more than $42,000 per violation.

[220] 15 U.S.C. § 45(n); *see also*, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), reprinted in International Harvester Co., 104 F.T.C. 949, 1070, 1073 (1984) ("Unfairness Policy Statement"). http://www.ftc.gov/bcp/policystmt/ad-unfair.htm,

[221] FTC Statement on Deception, 103 F.T.C. 174, 175 (1984) (appended to Cliffdale Assocs., Inc., 103 F.T.C. 110 (1984)) ("Deception Policy Statement").

[222] *Id.*

material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception. In many instances,
materiality, and hence injury, can be presumed from the nature of the practice. In other instances, evidence of materiality may be necessary.[223]

As noted above, diverse civil remedies may be implicated for unfair or deceptive acts or practices relating to privacy (or otherwise), and for violations of Commission orders, or of rules implementing either Section 5 or special statutes pertinent to privacy, such as COPPA.[224] Such remedies include, but are not limited to, harm-based remedies. First, Section 13(b) of the FTC Act, authorizes the Commission to seek preliminary and permanent injunctions to remedy "any provision of law enforced by the Federal Trade Commission,"[225] and such injunctions may require diverse behavioral remedies tailored to the parties and their conduct.[226] Second, Section 19 of the FTC Act,[227] authorizes the Commission to file suit in United States District Court to enjoin an act or practice that is in violation of any provision of law enforced by the FTC. Such injunctions may comprise temporary restraining orders, preliminary injunctions, or "in proper cases," permanent injunctions proscribing the violative conduct. In addition, although the FTC Act does not generally authorize claims for civil money damages for initial violations of Section 5, Section 19 of the FTC Act provides that monetary penalties may apply to knowing violations of Commission orders, or to violations of FTC regulations regarding unfair or deceptive practices, including rules under special privacy statutes, such as the COPPA rule.[228] Such penalties may include "the refund of money or return of property . . . [and] the payment of damages," in addition to equitable relief such as the recission or reformation of

---

[223] *Id.*

[224] *See, e.g.*, Fed. Trade Comm'n, Privacy & Data Security Update: 2019 (2020), https://www.ftc.gov/reports/privacy-data-security-update-2019.

[225] 15 U.S.C. 53(b)

[226] *See, e.g.*, Fed. Trade Comm'n, Privacy & Data Security Update: 2019, *supra* note 216.

[227] 15 USC 57(b).

[228] *Id.* Section 5 and Section 19 both stipulate statutory caps for monetary penalties per violation. Penalties initially stipulated in the FTC Act itself, as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. §2461, amended by the Federal Civil Penalties Inflation Adjustment Improvements Act of 2015, Public Law 114-74, sec. 701, 129 Stat. 599 (2015), and Section 1.98(d) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(d), authorizes civil monetary penalties of not more than $42,530 for each such violation of the Rule.

contracts. [229]

d. Soft Law: Guidance and Advocacy

The FTC's advocacy efforts, including competition advocacy, have an important role to play in data policy. Such advocacy is informative, and potentially persuasive, rather than an exercise of enforcement authority.[230] It is grounded in an application of economic principles and draws upon the FTC's enforcement experience. The agency's advocacy plays an important role given the ubiquity of both data and consumer data issues across the economy, the often significant interface of consumer data protections with competition and innovation, the benefits of disseminating competition expertise among diverse regulators, the relative stickiness or durability of competitive harms (often inadvertently) produced by laws and regulations, and the limited legal authority antitrust authorities often have over policy making that can significantly impact competition.[231] It has, as well, been widely regarded as an efficient means of policy development and adoption,[232] notwithstanding that assessing the impact of a given advocacy may be difficult.[233] Advocacy may be a form of "soft" intervention, but it is considerably less costly than litigation and often more general in its effects; and it has the potential to introduce or amplify competition and efficiency considerations into both federal and state policy making where federal antitrust authority is limited.[234]

---

[229] 15 USC 57(b).

[230] *See, e.g.*, James C. Cooper, Paul A. Pautler & Todd J. Zywicki, *Theory and Practice of Competition Advocacy at the FTC*, 72 ANTITRUST L.J. 1091, 1098 (2005); Maureen K. Ohlhausen, *Identifying, Challenging, and Assigning Political Responsibility for State Regulation Restricting Competition*, 2 *Comp. Pol'y Int.* 151 (2006); Daniel J. Gilman, *Advocacy*, SAGE ENCYCLOPEDIA OF POLITICAL BEHAVIOR 8 (Fathali M. Moghaddam, ed. 2017).

[231] The advocacy program, its rationale, and its effects are described variously in the articles cited in note 222, *supra*.

[232] *See, e.g.*, WILLIAM E. KOVACIC, (then) CHAIRMAN, FED. TRADE COMM'N, THE FEDERAL TRADE COMMISSION AT 100: INTO OUR SECOND CENTURY, 122 (2008), https://www.ftc.gov/sites/default/files/documents/public_statements/federal-trade-commission-100-our-second-century/080618ftcat100.pdf; Cooper, Pautler, & Zywicki, *supra* note 222, at 1110-1111.

[233] *See, e.g.*, Cooper, Pautler, & Zywicki, *supra* note 222, at 1110.

[234] *See supra* note 222.

The role of the FTC in such advocacy is distinctive, partly because of the FTC's role in both US antitrust enforcement and US privacy enforcement, and partly because the FTC Act, which establishes and authorizes the FTC, also gives the FTC a research, education, and policy mission. In particular, the FTC is to investigate and report on market developments in the public interest and make legislative recommendations based on its findings.[235] For example, FTC staff have advised sectoral regulators on competitive implications (possible benefits and harms) of interoperability policies, recognizing and advocating for consideration of "appropriate administrative, physical, and technical safeguards … to ensure the confidentiality, integrity, and security of consumers' data."[236] In doing so, agency staff identified potential pro-competitive advantages to enhanced interoperability and both public and private standard-setting endeavors, such as lower switching costs and reduced barriers to entry. At the same time, staff elucidated certain trade-offs in such endeavors,[237] noting that the likelihood and magnitude of benefits and costs are often context and implementation specific.[238] The staff also identified potential competitive concerns, including anticompetitive conduct sometimes associated with standard setting.[239]

---

[235] Section 6 of the FTC Act, 15 USC 46, gives the Commission the authority to conduct investigations in the service of FTC enforcement actions, but also provides a more general authority to investigate and report on market developments in the public interest; and it gives the Commission the authority to make legislative recommendations based on those investigations. *Id.* at § 46(b), (f).

[236] Fed. Trade Comm'n Staff Comment Before the Office of the National Coordinator for Health Information Technology, regarding Its Draft Shared Nationwide Interoperability Roadmap for Health Information Technology Systems (Apr. 2015), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staffcomment-office-national-coordinator-health-information-technology-regarding-its-draft/1504-roadmaphealth.pdf. The staff commended ONC and HHS for their consideration of appropriate measures to be taken by HIPAA-covered entities, including encryption, contractual requirements on business partners, incident response capabilities, and strong authentication policies. At the same time the staff comment noted the need for appropriate protections for, e.g., personal health information held by non-HIPAA-covered entities, citing various FTC enforcement matters where firms had failed to implement such safeguards. *Id.*

[237] Broadly, "[t]he coalescence of industry around particular standards trades off reduced intersystem competition for increased intrasystem competition. Intersystem competition takes place when firms that employ different standards compete in the marketplace. Intra-system competition, in contrast, takes place between firms that have adopted the same standard." *Id.* at 11 (citations omitted).

[238] *Id.* at 9. Staff also noted that "the effects of standardization on competition are complicated and may have unintended consequences." *Id.*

[239] Staff cited examples of, e.g., improperly refusing to certify a competitor's product as standard compliant, improperly refusing to adopt or amend a standard to include innovative products developed after the standard was adopted, improperly adding members to a SSO to influence its voting, and improperly failing to

Other advocacies addressed both competition and consumer privacy issues implicated in national "information blocking" and certification regulations for health information and health IT, where the statute being implemented had expressly recommended consultation with the FTC, as acknowledged by formal FTC staff comments and the HHS NPRM.[240] Staff have noted, for example, that antitrust tends to impose duties to deal (in information or otherwise) only under certain circumstances, given the risks to fundamental mechanisms of market pricing, competition, and innovation, as well as risks to data privacy and security, posed by overbroad or undue obligations to share personal information. FTC staff have also had input into, e.g., the balancing of consumers' interests in privacy, competition, and innovation in a national telecommunications policy.[241]

e. Artificial Intelligence

Recent developments in A.I., including those in Generative A.I. and, specifically, L.L.M.s, underscore the promise of the data economy and large data sets.[242] At

disclose the existence of patent rights relevant to technology being considered for inclusion into a standard. *Id.* at 7-8.

[240] FTC Staff Letter to Department of Health and Human Services Concerning the 21st Century Cures Act: Interoperability, Information Blocking and the ONC Health IT Certification Program Rule (Mar. 2020), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-letter-department-health-human-services-concerning-21st-century-cures-act-interoperability/v190002hhsinfoblockingletter.pdf; FTC Staff Comment Before the Dep't of Health & Human Servs. Regarding the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (2019), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-department-health-human-services-regarding-21st-century-cures-act-interoperability/v190002_hhs_onc_info_blocking_staff_comment_5-30-19.pdf.

[241] FTC Staff Comment to the NTIA: Developing the Administration's Approach to Consumer Privacy (2018), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

[242] Although there is no canonical definition of "Generative A.I.," a recent report by the Congressional Research Service provides a useful, if brief, overview. U.S. Cong. Res. Serv., Generative Artificial Intelligence and Data Privacy: A Primer, R47569, 1-3 (May 23, 2023) https://crsreports.congress.gov/product/pdf/R/R47569. And as noted therein, the National Artificial Intelligence Initiative Act of 2020 (P.L. 116-283) defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—(A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action."

the same time, scraping and other automated means of mass data collection employed to provide inputs into Generative A.I. have raised privacy concerns,[243] and, indeed, the prospect and onset of new regulation.[244] While we cannot gainsay the potential for consumer harm, we can suggest that some of that harm may be addressed by extant regulation. As the Joint Statement observes, A.I. applications *in commerce* are, already, subject to the FTC Act, including Section 5's prohibition of unfair and deceptive acts or practices, among other regulations.[245]

In addition, policy makers should be mindful of the fact that this is a burgeoning field, comprising diverse technologies and applications. These implicate the potential for – and increasing delivery of – consumer benefits, and not just potential harm. At the highest level, policy initiatives ought to be evidence-based; they ought to account for consumer benefits as well as potential harms, as should privacy policy more broadly; and they ought to produce net benefits to consumer welfare. A risk-based approach, therefore, ought to follow risk management principles, accounting for likely and demonstrable benefits, likely and demonstrable harms, and – based on best evidence – the likelihood, magnitude, and likely timing of such benefits and harms. For policy to confer consumer welfare benefits *on net* – consistent with established antitrust principles and the FTC's unfairness authority – it is insufficient to merely catalogue possible (and conjectured) harms. Doing so can be a

---

[243] Generative Artificial Intelligence and Data Privacy, supra note 33, at 4-5.

[244] *Id.* at 6-7. For example, in April 2023, the FTC, U.S. Dep't Justice Civil Rights Commission, Consumer Financial Protection Bureau (CFPB), and Equal Employment Opportunity Commission Released a Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems, https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/joint-statement-enforcement-efforts-against-discrimination-bias-automated-systems. Bills introduced in the current (118th) Congress include, e.g., the AI Disclosure Act of 2023, H.R. 3831, 118th Cong (2023). We note, in Europe, the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SEC (2021) 167 final (Apr. 21, 2021). And in October 2022, the White House Office of Science and Technology Policy published a Blueprint for an AI Bill of Rights, identifying "five principles that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence." https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf. Although the Blueprint does not itself comprise an Executive Order, it is likely to influence diverse regulatory decisions under the Biden Administration, at least.

[245] Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems, *supra* note 37.

useful issue-spotting exercise, but without further analysis, it is a slim basis on which to impose significant costs on pro-consumer applications and development.

In that regard, we note that the recent Blueprint for an A.I. Bill of Rights is in some respects appropriately general and flexible, as it eschews specific regulatory recommendations and takes note of the developing nature of the field. At the same time, elements of the Blueprint recall the sweep and imbalance of the FTC's ANPR on "Commercial Surveillance and Data Security," which barely nodded to the consumer welfare tradeoffs implicated in privacy policy, over-emphasizing potential harms and under-emphasizing both demonstrated consumer benefits and an empirical basis for regulation.[246] In addition, the Blueprint mirrors attributes of GDPR that have been associated with diverse and substantial costs but few demonstrated consumer benefits. For example, the Blueprint states that

> Data collection should be limited in scope, with specific, narrow identified goals, to avoid "mission creep." Anticipated data collection should be determined to be strictly necessary to the identified goals and should be minimized as much as possible." . . . Clear timelines for data retention should be established, with data deleted as soon as possible in accordance with legal or policy-based limitations. Determined data retention timelines should be documented and justified.[247]

While that does not specify a regulatory requirement, it recalls GDPR's data minimization requirements in a way likely to be costly for innovation and, specifically, for data intensive model and application development. Similarly, the Blueprint's discussion of consumer "data access and correction,"[248] and for "consent withdrawal and deletion,"[249] recall, and in some ways exceed, GDPR requirements for consumer control in ways that may be particularly difficult to implement with systems trained on large and complex datasets. To

---

[246] See text accompanying notes 9 - 10, *supra*; Manne, Gilman & Stout, note 10, *supra*.
[247] AI Blueprint, supra note 37, at 33.
[248] *Id.* at 35.
[249] *Id.*

emphasize, we do not argue that there cannot be contexts in which some aspects of these "rights" might be appropriate. Rather, we suggest that the empirical literature, most recently on GDPR, suggests caution, and that the development of any such restrictions be conducted with attention to the costs and benefits of regulation as well as the costs and benefits of commercial conduct.

IV. Conclusion

Privacy research – theoretical and empirical – remains both a fruitful area of inquiry and a work in progress. As the preceding discussion illustrates, privacy is conceptually complex, rather than a simple state-of-affairs or a uniform attribute of goods and services. Moreover, privacy is a domain in which the costs and benefits – both demonstrated and potential – are heterogenous, and may vary across industries, data domains, or types of regulatory intervention, and not just across persons. From a policy standpoint, privacy is not a simple goal or function to be optimized – and privacy policies may entail especially complex tradeoffs. Those tradeoffs can vary across consumers (patients, citizens, etc.); and they can vary across contexts for any given individual as well. Empirical research on privacy – and on the economic impact of privacy and related data regulations – illustrates some of the complex tradeoffs implicated in privacy policy reform. Potential costs are not simply compliance costs, although those can be substantial. They can include, among other things, tradeoffs between privacy protections and the flow of information – and consequently, between privacy protections and the consumer benefits that the flow of information may enable. They can entail tradeoffs between consumer control over and access to information, and between privacy and data security. Privacy policies may have unintended consequences; they can impede innovation, and they can harm competition, to the extent that they burden small innovative firms and would-be entrants to a greater degree than they do incumbents, firms with multiple product lines, and firms with a relatively large installed base.

That is not to say that there is nothing for policy makers to do. Information costs regarding the collection, use, and transfer of consumer data remain high; and information asymmetries appear common and persistent. Demonstrable harms are substantial – at least in aggregate – even on the narrowest conception of consumer harm.

Hence, the diverse interests that constitute privacy pose distinctive challenges, as well as opportunities, for policymakers. Major regulatory initiatives have been undertaken – and continue to be considered – without anything like fulsome, much less comprehensive, consideration of their likely costs and benefits, and the impact of regulation on competition seems consistently given short shrift. Cost-benefit analysis of the HIPAA Privacy Rule[250] – a regulation that applies to much of the collection, storage, use, and transfer of digital health information that has led to tens of thousands of enforcement investigations[251] – was admittedly limited from the start. In its 1999 Notice of Proposed Rulemaking,[252] the Department of Health and Human Services acknowledged that its "ability to measure costs of the proposed regulation is limited because there is very little data currently available on the cost of privacy protection . . . [and HHS] has not been able to estimate costs for a number of requirements of the proposed regulation that we know will impose some cost to covered entities."[253] Even acknowledged compliance costs were not fully accounted for, and indirect costs and competitive impact seem not to have been considered at all. Estimated costs – notwithstanding acknowledged lacunae in the Department's analysis – were roughly $3.8 billion for five years.

A recent wide-ranging legislative proposal in the U.S. – the American Data Privacy and Prevention Act (ADPPA)[254] – was not adopted during the 117th Congress, despite

---

[250] The HIPAA Privacy Rule is codified at 45 C.F.R. Part 160 and Subparts A and E of Part 164. Attendant discussion was included with the publication of the final rule in the Federal Register. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182, Aug. 14, 2002 (to be codified at 45 C.F.R. Parts 160 – 164).

[251] *See* note 85, *supra*.

[252] Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918 (proposed Nov. 3, 1999) (to be codified at 45 C.F.R. Parts 160 – 164).

[253] *Id.* at 6006-6008.

[254] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2021-22).

considerable attention and bipartisan support. It may well be reintroduced in the 118th Congress, and may be instructive in any case, to the extent it illustrates policy considerations that have at least some degree of traction in the United States and elsewhere.[255] Like the EU's GDPR, the ADPPA aspired to be a general data privacy law – one ranging across industry sectors and types of data and applications. Notably, the ADPPA incorporated some of the same types of provisions as the GDPR.

Both the ADPPA and the GDPR range over very broad definitions of "personal data" or "covered data," and both incorporate heightened restrictions for certain sensitive data. Both include transparency requirements; and both include broad data minimization requirements. Under the ADPPA, as a "covered entity" would not be able to "collect, process, or transfer covered data unless the collection processing or transfer is limited to what is reasonably necessary and proportionate to (1) provide or maintain a specific product or service requested by the individual to whom the data pertains; or (2) effects . . . [an enumerated permitted purpose].[256] Enumerated permitted purposes include, for example, those "necessary to perform system maintenance or diagnostics," "to protect against spam," "to debug or repair errors that impair the functionality of *a service or product for which such data was collected,"* and the fulfillment of a product or service warranty.[257] In addition, the ADPPA requires express consent for the collection, use, and transfer of "covered data";[258] and like the GDPR, the ADPPA would permit consumers broad latitude in withdrawing consent that's been given. The ADPPA's provision granting consumers the right to have "covered data" deleted under Section 203 is in some regards stronger than "the right to be forgotten" under the GDPR; and both include rights of access

---

[255] For an overview of the ADPPA's provisions, see, e.g., Cong. Res. Serv., Overview of the American Data Privacy Protection Act, HR 8152 (updated Aug. 31, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776.

[256] ADPPA, Section 1: Data Minimization.

[257] *Id.* Under GDPR, data minimization provisions require that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed," and must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."

[258] Certain EU consent requirements were imposed pre-GDPR through the 2002 EU Privacy Directive. And in some ways, the consent requirements under the ADPPA are stronger than those in force under the GDPR.

and rectification. The GDPR requires organizations to appoint a Data Protection Officer; and the ADPPA would require covered entities or service providers with 15 or more employees to have both "1 or more qualified employees as privacy officers; and … 1 or more qualified employees (in addition to any employee designated under subparagraph (A)) as data security officers."[259]

Of course, the ADPPR does not simply recapitulate the provisions of the GDPR – there are differences as well as similarities; and effects might vary not just according to regulatory provisions, but their implementation, and the environment (or jurisdiction) in which they apply. Still, the similarities seem significant: very wide-ranging data regulations conferring substantial rights or entitlements on consumers or "data subjects," with stringent limitations on data use, transfer, and retention, and costly compliance mandates, such as the designation or appointment of privacy or data protection officers by firms handling personal data. Despite the broad sweep of the ADPPA and the GDPR, neither the U.S. bill nor the E.U. regulation seems to have been drafted with any significant awareness of – much less accounting for – the complex tradeoffs that may be implicated by privacy regulations. And neither seems to have been predicated on a thoroughgoing cost-benefit analysis.

As we saw above, the literature on the economic impact of GDPR suggests that policy makers ought to be cautious in proposing general or cross-sector data regulations. Many in Europe had proposed—or conjectured—that GDPR would be "an enabler of competition."[260] For example, at an FTC hearing on Big Data, Privacy, and Competition, Rainer Wessely, from the Delegation of the European Union to the U.S., reviewed several possible competitive advantages to the European approach and GDPR, concluding that, "eventually the GDPR should stimulate innovation and competition."[261] We have reviewed a

[259] ADPPA, Section 301(c)(1).

[260] Fed. Trade Comm'n, Hearings on Competition and Consumer Protection in the 21st Century, Big Data, Privacy, and Competition (Nov. 6-8, 2018) at 269 (testimony of Renato Nazzini), https://www.ftc.gov/system/files/documents/public_events/1418633/ftc_hearings_session_6_transcript_day_2_11-7-18_1.pdf.

[261] *Id.* at 290 (testimony of Rainer Wessely).

number of studies indicating harms to competition and innovation that have been associated with GDPR. That evidence is mounting; and while we do not consider such research comprehensive, we are unaware of credible systematic studies demonstrating that GDPR has produced countervailing benefits for competition or consumers, such as reduced consumer harm, lower risk of identity theft, or enhanced entry or innovation etc. Early suggestions from Europe of competitive benefits[262] may someday, to some extent, and in some regards, be substantiated, but thus far, they run contrary to the available evidence.

There may, of course, be some advantages to relatively broad data regulations. In the U.S. at least, uniform federal regulations (with preemption of state law) could have the advantages of uniformity and predictability. And we do not imagine that there is no further demand for privacy regulation. There is, however, the potential misfit between very broad rules, heterogeneous regulated conduct, and heterogenous policy goals. More specifically, some of the ADPPA provisions that mirror GDPR provisions – such as data minimization, the appointment of a privacy officer, and the frequency of required opt-in – may differentially burden small innovative firms and would-be entrants, relative to incumbents, firms with multiple product lines, and firms with a relatively large installed base.

We suggest at least a modicum of research-based caution with regard to both federal legislative proposals like the ADPPA and federal regulatory proposals, such as that undertaken by the FTC's ANPR on "Commercial Surveillance" and Data Security.[263] A laundry list of concerns about harms, actual and potential, clear and ambiguous, estimable and otherwise, does little to inform policy makers who would consider the tradeoffs entailed by reform in a careful way. Despite the FTC's considerable enforcement experience with privacy matters – and the research expertise of its Bureau of Economics – the FTC's

---

[262] *See id.* (testimony of Rainer Wessely); *cf*. Marco Botta & Klaus Wiedemann, *The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*, 64 Antitrust Bulletin 428 (2019) (recognizing different goals of competition and consumer protection law, but also maintaining that "[a] number of provisions contained in the GDPR aim at tackling a number of market failures in digital markets, such as those requiring the data subject's "informed" consent. In addition, by sanctioning misleading and aggressive commercial practices, consumer law also safeguards the final consumer's "informed" choice.).

[263] ANPR, *supra* note 2.

ANPR seems to pay only nominal attention to such tradeoffs. Although the ANPR takes some notice of the costs of identity theft, it fails to identify the specific types of harm FTC regulation might address, much less to estimate the magnitude of such harms. Indeed, the 129 footnotes to the ANPR contain precisely zero direct references to the primary research literature.[264] And as comments submitted to the regulatory record by the International Center for Law and Economics put it, the ANPR "provides a laundry list of putative harms, and it fails to identify even the most basic benefits that may be associated with diverse commercial data practices."[265]

That seems a failing in several respects: first, it undercuts the FTC's ability to adopt privacy regulations under its "unfairness" authority that prohibit – effectively, efficiently, or otherwise – acts or practices that cause or are "likely to cause substantial injury to consumers" that are "not outweighed by countervailing benefits to consumers or to competition," as required by statute;[266] second, it impedes the FTC's ability to adopt privacy regulations that accomplish what the unfairness prong of Section 5 of the FTC Act requires; that is, regulations (including enforcement standards and remedies) that address substantial consumer harms, and that are, on net, beneficial to consumers; third, it leaves aside important research that the FTC is well-equipped to develop: namely, establishing a theoretical and empirical basis for such regulations. That would include, but not be limited to, research regarding the benefits of various privacy regulations, so that hard policy questions about data regulation can be answered in an informed way. The high-level takeaway from the privacy literature is that of the ubiquity of significant tradeoffs; the policy implication is that the details matter for effective and efficient policy, and that there's a great deal at stake.

---

[264] There is one indirect reference to a working paper, via citation to a newspaper article covering the putative findings of that study.

[265] Geoffrey A. Manne, Daniel J. Gilman & Kristian Stout, Comments of the International Center for Law & Economics: FTC Advance Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, Docket No. FTC-2022-0053, Commercial Surveillance ANPR, R111004, Nov. 22, 2022, tinyurl.com/ycx4vk8f.

[266] 15 U.S.C. § 45(n).