SAFETY AS PRIVACY

A. Michael Froomkin, Phillip J. Arencibia,
and P. Zak Colangelo-Trenner[***]

New technologies, such as internet-connected home devices we have come to call the Internet of Things (IoT), connected cars, sensors, drones, internet-connected medical devices, and workplace monitoring of every sort, create privacy gaps that can cause danger to people. In prior work,[1] two of us sought to emphasize the deep connection between privacy and safety to lay a foundation for arguing that U.S. administrative agencies with a safety mission can and should make privacy protection one of their goals. This Article builds on that foundation with a detailed look at the safety missions of several agencies. In each case, we argue that the agency has the discretion, if not necessarily the duty, to demand enhanced privacy practices from those within its jurisdiction and that the agency should make use of that discretion.

Armed with the understanding that privacy is or causes safety, several U.S. agencies tasked with protecting safety could achieve substantial gains to personal privacy under their existing statutory authority. Examples of agencies with untapped potential include the Federal Trade Commission ("FTC"), the Consumer Product Safety Commission ("CPSC"), the Food and Drug Administration ("FDA"), the National Highway Traffic Safety Administration ("NHTSA"), the Federal Aviation Administration ("FAA"), and the Occupational Safety and Health Administration ("OSHA"). Five of these agencies have an explicit duty to protect the public against threats to safety (or against risk of injury) and thus—as we have argued previously—should protect the public's privacy when the absence of privacy can create a danger. The FTC's general authority to fight unfair practices in commerce enables it to regulate commercial practices threatening consumer privacy. The FAA's duty to ensure air safety could extend beyond airworthiness to regulating spying via drones.

*** A. Michael Froomkin, Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law, University of Miami, Fellow, Yale Information Society Project, Member, Miami Center for Computational Science (Professor Froomkin discloses that he advised EPIC in the *EPIC v. FAA* case, *infra* note 398); Phillip J. Arencibia, Attorney, Duane Morris LLP, Miami, Florida; P. Zak Colangelo-Trenner, Attorney, Hamilton, Miller & Birthisel, LLP, Miami, Florida. We would like to thank Caroline Bradley, David Froomkin, Woody Hartzog, Andrea Matwyshyn, Gabe Scheffler, Alicia Solow-Niederman, Paul Schwartz, and participants at a presentation in the 2021 Privacy Law Scholars Conference.

1. A. Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 WASH. L. REV. 141 (2020).

The CPSC's authority to protect against unsafe products authorizes it to regulate products putting consumers' physical and financial privacy at risk, thus sweeping in many products associated with the IoT. NHTSA's authority to regulate dangerous practices on the road encompasses authority to require smart car manufacturers to include precautions protecting drivers from misuses of connected car data due to the carmaker's intention and due to security lapses caused by its inattention. Lastly, OSHA's authority to require safe work environments encompasses protecting workers from privacy risks that threaten their physical and financial safety on the job.

Arguably, an omnibus federal statute regulating data privacy would be preferable to doubling down on the United States' notoriously sectoral approach to privacy regulation. Here, however, we say only that until the political stars align for some future omnibus proposal, there is value in exploring methods that are within our current means. It may be only second best, but it is also much easier to implement. Thus, we offer reasonable legal constructions of certain extant federal statutes that would justify more extensive privacy regulation in the name of providing enhanced safety, a regime that we argue would be a substantial improvement over the status quo yet not require any new legislation, just a better understanding of certain agencies' current powers and authorities. Agencies with suitably capacious safety missions should take the opportunity to regulate to protect relevant aspects of personal privacy without delay.

TABLE OF CONTENTS

INTRODUCTION

New technologies, such as the Internet of Things ("IoT") and connected cars, create privacy gaps that can cause dangers to people. In a previous article, *Privacy as Safety*,[2] two of us sought to emphasize the deep theoretical connection between privacy and safety. As promised there, we turn now to how, in practice, legislation that protects safety can be harnessed to protect privacy. Many agencies have consumer-protection or safety missions. We argue that the safety objectives of several U.S. agencies permit, even if they do not necessarily require, those agencies to issue rules requiring enhanced privacy practices and protections from those within their jurisdictions. To our knowledge, this is the first article in the legal literature to identify the substantial gains to personal privacy that U.S. agencies tasked with protecting safety could achieve under their existing statutory authority. We also give suggestions of where specifically each of six agencies might begin.

Many U.S. agencies tasked with protecting safety could and should be doing more to protect personal privacy. Examples of agencies with untapped potential include the Federal Aviation Administration ("FAA"), the Federal Trade Commission ("FTC"), the Consumer Product Safety Commission ("CPSC"), the National Highway Traffic Safety Administration ("NHTSA"), and the Occupational Safety and Health Administration ("OSHA"). Each of these agencies has a duty to protect the public against threats to safety and thus—as we have argued previously—could choose to protect the public's privacy when the absence of privacy can create a danger.

The FTC's general authority to fight unfair practices in commerce enables it to regulate commercial practices threatening consumer privacy; while the FTC has

2. *Id.*

penalized some egregious practices,[3] it has not yet exercised its power to make broader rules protecting consumer privacy. The FAA's duty to ensure air safety could extend beyond airworthiness to regulating spying via drones.[4] The CPSC's authority to protect against unsafe products authorizes it to regulate products putting consumers' physical and financial privacy at risk, thus sweeping in many products associated with the IoT. NHTSA's authority to regulate dangerous practices on the road encompasses the authority to require connected-car manufacturers to include precautions protecting drivers from hacker interference with control of connected cars and from misuses of connected-car data. Lastly, OSHA's authority to require safe work environments encompasses the authority to protect workers from privacy risks that threaten their physical and financial safety on the job.

Some have argued that an omnibus federal statute regulating data privacy would be preferable to doubling down on the United States' notoriously sectoral approach to privacy regulation.[5] We are inclined to agree. Here, however, we say only that until the political stars align for some future omnibus proposal, there is value in exploring methods that are within our current means. It may be only second best, but we offer reasonable legal constructions of certain existing federal statutes that would justify more extensive privacy regulation in the name of providing enhanced safety, a regime that we argue would be a substantial improvement over the status quo yet not require any new legislation, just a better understanding of certain agencies' current powers and authorities. Indeed, even if Congress can pass a limited privacy bill,[6] there may still be much need, and much scope, for complementary agency action based on existing authority.

We begin Part I of this Article with a brief summary of the arguments in our companion piece, *Privacy as Safety*. In particular, we review the argument that agencies can further their safety aims through privacy regulation. We then turn to the United States' lack of comprehensive privacy regulation, whether through legislation or agency action. We then explain what it means that the U.S. approach to privacy is sectoral rather than omnibus. Part I concludes with a call to action, urging agencies with suitably broad safety mandates to take the opportunity to regulate to protect relevant personal privacy without delay.

Part II surveys six agencies' statutory authority and explains how their authority enables the agencies to act within the privacy sphere. We distinguish between inability and mere unwillingness to act. Each section concludes with some specific examples of privacy-enhancing actions that the agency could undertake with its current authority. We make no claim that these lists are exhaustive; on the contrary, they are better understood as low-hanging fruit.

Part III is a very brief conclusion.

---

3. *See infra* Section II.B.1.

4. Two of us also previously examined some of the privacy, and thus safety, threats posed by drones. *See generally* A. Michael Froomkin & P. Zak Colangelo, *Self-Defense Against Robots and Drones*, 48 CONN. L. REV. 1 (2015).

5. *See infra* note 44.

6. *See infra* text accompanying notes 232–37 (discussing proposed American Data Privacy and Protection Act).

I. USING 'PRIVACY AS SAFETY' TO PLUG HOLES IN UNITED STATES' PRIVACY LAW

A. Privacy as Safety in a Nutshell

Privacy as Safety argued that in many circumstances, privacy makes you safer[7] in broad and overlapping ways: "(1) it makes one physically safer; (2) it provides psychological security; (3) it makes one economically safer (and protects from some forms of invidious discrimination); and (4) it makes the exercise of various political rights safer."[8]

Privacy as Safety identified a wide range of circumstances in which U.S. law already protects privacy as a means of protecting safety. Protecting locational privacy is a means of protecting physical safety, as seen from witness-protection programs and laws that hide the sensitive personal information of judges, police officers, and jurors.[9] U.S. law has rules that safeguard personal information to protect against abusers, kidnappers, stalkers, doxxers, and swatters; it even has rules that permit sheltering lottery winners from potentially harmful publicity.[10] Perhaps most fundamentally, *Privacy as Safety* canvassed legal protections of spatial privacy—the law's recognition of a person's interest in the privacy of particular physical locations, primarily those locations the person considers intimate.[11] The right to exclude unwanted intrusion in an area a person identifies as theirs carries clear benefits for physical, psychological, and economic safety. Similarly, protection of communicational privacy in nonintimate contexts, such as in whistleblower-protection rules, protects the physical and economic safety of the whistleblower by guarding against reprisals.[12]

Privacy as Safety also identified "privacy gaps," areas where safety is threatened by a lack of privacy regulation.[13] New technologies—like the IoT, social media, and drones—illustrate reductions in privacy that expose people to new dangers. The IoT and drones expose users (and those nearby) to surveillance, potential manipulation, and disclosure of intimate facts. Social media allows intermediaries to collect volumes of personal data about both account holders and their friends. People also use social media to effectively spy on themselves, prompting questions about what sort of regulation, if any, would protect their privacy and their safety.

By advancing a surprisingly dormant argument that privacy enhances safety, *Privacy as Safety* sought to lay the foundation for claims that U.S. administrative agencies with a safety mission can and should make privacy

---

7. Froomkin & Colangelo, *supra* note 1, at 141.

8. *Id.* at 163. *Privacy as Safety* also noted, but did not fully explore, the idea that "[a]rguably, by reducing stress caused by surveillance and other invasions of privacy, it also makes one safer from illness." *Id.* at 163 n.107.

9. *Id.* at 163–67.

10. *Id.* at 167–75.

11. *Id.* at 177.

12. *Id.* at 179–86.

13. *Id.* at 195–202.

protection one of their goals.[14] Below, we seek to redeem the promise made in *Privacy as Safety* by taking a detailed look at the safety missions of several agencies. In each case, we argue that the agency has the discretion, if not the duty, to demand enhanced privacy practices from firms within its jurisdiction, and we give examples of benefits that would follow if the agency would make a commitment to enhancing personal privacy as a part of its safety mission.

B. The United States' Approach to Privacy Regulation

1. Sectoral v. Omnibus Regulation

The United States does not have European Union-style omnibus privacy legislation[15] like the General Data Protection Regulation ("GDPR").[16] Nor does it have a federal agency responsible for privacy issues, generally.[17] Rather, the United States takes a sectoral approach: "federal U.S. privacy statutes do not cover all personal data, but only data in particular sectors, or held by particular entities."[18] While these rules overlap in places, the laws are generally narrow and targeted, aiming at particular sectors of industry and imposing special, industry-specific rules. Even where U.S. laws take a broader approach, they remain limited, or sectoral, in nature. For example, many U.S. privacy laws take "a *consumer protection* approach, . . . focusing on protecting individuals in direct relationships with companies."[19] That is, "data privacy protections in the United States largely extend only so far as direct consumer relationships, and not to the growing variety of both surveillance systems and data processing conducted by third parties that have no direct relationship to consumers."[20]

In contrast, "[t]he core of any omnibus bill is a reliance on general clauses."[21] General clauses implement privacy norms in a manner not tailored to a specific area of information processing but rather in a manner hoped or expected to be generally applicable to the full range of potential privacy issues. As Meg Letta Jones and Margot Kaminsky explain, this is the GDPR's approach, and its reliance on imposing "broad standards rather than specific rules" can be "befuddling" to U.S.

---

14. *Id.* at 141.

15. *But see infra* text accompanying notes 232–37 (discussing proposed American Data Privacy and Protection Act).

16. *See* Regulation 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), 2016 O.J. (L 119) 1(EU) [hereinafter GDPR].

17. For an argument in favor of creating a single federal agency charged with monitoring, but not regulating, privacy issues, see Robert Gellman, *New Models: A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183, 1183 (2003). *See also* Omar Saleem, *The Establishment of a U.S. Federal Data Protection Agency to Define and Regulate Internet Privacy and its Impact on U.S.–China Relations: Marco Polo Where Are You?*, 19 J. MARSHALL J. COMPUTER & INFO. L. 169 (2000).

18. Meg Leta Jones & Margot E. Kaminsky, *An American's Guide to the GDPR*, 98 DENVER. L. REV. 93, 106–07 (2020).

19. *Id.* at 107.

20. *Id.*

21. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 911 (2009).

readers used to the regime that commonly seeks greater specificity.[22] Jones and Kaminsky emphasize that the GDPR is "written in many places in broad, almost aspirational terms—the kind of language that gives U.S. compliance lawyers serious heartburn. But that vagueness is at least partially intentional. The GDPR is often vague because it tasks companies with figuring out how to best implement its aspirations."[23] The GDPR, they explain, is a "process rather than a set of clear legal requirements."[24] In this way, and in reliance on a compliance rather than enforcement regime, the GDPR manages to protect data, regardless of who holds it.

As the GDPR is necessarily broader than the United States' sectoral, largely consent-based regime, the GDPR's strictures apply regardless of whether an individual invokes a privacy right.[25] In addition to limiting itself to a sectoral approach to privacy, the United States has long been criticized for an "excessive focus on individual notice and choice."[26] The U.S. notice- and consent-based system is "based on long, elaborate privacy policies—that often go unread—and surveillance that is impossible to opt out of in practice."[27]

In contrast, the GDPR requires that data be "processed lawfully," and begins by banning the processing of personal data unless a lawful condition applies.[28] Article 6 of the GDPR then lays out the lawful conditions: individual consent; necessity for the performance of a contract; necessity for compliance with a legal obligation; necessity to protect the vital interests of the subject or another person; necessity for a task carried out in the public interest; or necessity for the "legitimate interest" of the data controller, "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[29]

The United States' sectoral approach to privacy has its roots in state common law, especially tort law's protection of the right to privacy.[30] As Robert C. Post famously noted, "tort privacy is centered on civility norms that maintain and structure communal life."[31] But tort law's protection of privacy norms is weakening in light of communities' demand for accountability and open access to information, and the rise of surveillance in the information age—developments that have fundamentally altered communities' expectations regarding privacy and civility.[32]

---

22. Jones & Kaminsky, *supra* note 18, at 96.
23. *Id.* at 110.
24. *Id.* at 96.
25. *Id.* at 109.
26. *Id.* at 107 (citing Ian Kerr, *Devil is in the Defaults*, 4 CRIT. ANALYSIS L. 91, 98–99 (2017); Ian Kerr et al., *Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent*, in LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 1, 2, 6 (Ian Kerr et al. eds., 2009)).
27. *Id.* at 107–08.
28. GDPR, *supra* note 16, at art. 5(1)(a).
29. *Id.* at art. 6(1)(a)–(f).
30. Schwartz, *supra* note 21, at 907.
31. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989).
32. *Id.* at 1009–10; Schwartz, *supra* note 21, at 907.

The legal response to these changing norms began with the creation of the Fair Information Practices ("FIPs" or sometimes "FIPPS").[33] As summarized by Paul Schwartz, "[t]he basic toolkit of FIPs includes the following:

> (1) limits on information use; (2) limits on data collection, also termed data minimization; (3) limits on disclosure of personal information; (4) collection and use only of information that is accurate, relevant, and up-to-date (data quality principle); (5) notice, access, and correction rights for the individual; (6) the creation of processing systems that the concerned individual can understand (transparent processing systems); and (7) security for personal data.[34]

Although they were invented by a U.S. agency, the Department of Health, Education, and Welfare, the U.S. government never promulgated the FIPs in a unified or comprehensive privacy regulation. Rather, at least in the United States, "FIPs have generally developed through laws that regulate information use exclusively on a sector-by-sector basis."[35] The U.S. Privacy Act of 1974 is to some extent a general or omnibus privacy law, but it regulates only the public sector and is further limited in that it regulates only certain types of federal agencies and only certain types of data use.[36]

Given the United States' system of federalism, the lack of a comprehensive privacy regulation at the federal level has left states free to maneuver.[37] According to Paul Schwartz, "[t]he influence of state privacy law has been felt in three ways."[38] First, as the proverbial "boots on the ground," states "have often been the first to identify areas of regulatory significance and take action."[39] Second, states have been

---

33. The FIPs originated in a 1973 report of the HEW Secretary's Advisory Committee on the Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*. *See generally* Robert Gellman, *Fair Information Practices: A Basic History* – Version 2.22 (Apr. 6, 2022), http://ssrn.com/abstract=2415020 [https://perma.cc/4APR-SLN2].

34. Schwartz, *supra* note 21, at 908.

35. *Id.* at 910.

36. *Id.*

37. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016).

38. Schwartz, *supra* note 21, at 917.

39. *Id.* In the absence of federal privacy regulation, states have enacted their own comprehensive privacy laws. California enacted the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100, *et seq* (2018). California voters then added provisions to it by passing Proposition 24 in 2020. *See* California Privacy Rights Act of 2020 CAL. CIV. CODE § 1798.100 (2020), https://oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf [https://perma.cc/5RX6-3W2Q]; State Ballot Measures – Statewide Results, Cal. Sec'y St., https://electionresults.sos.ca.gov/returns/ballot-measures [https://perma.cc/46DH-UWV9] (last visited Oct. 27, 2022). Subsequently, Virginia enacted its Consumer Data Protection Act of 2021, VA. CODE ANN. §§ 59.1-196 to 207, https://lis.virginia.gov/cgi-bin/legp604.exe?ses=212&typ=bil&val=sb1392 [https://perma.cc/PV86-UBVU]. Also in 2021, Colorado enacted SB 190, the Protect Personal Data Privacy Act, COLO. REV. STAT. ANN. § 6-1-1301. Proposals for similar bills exist in several other states. *See* Taylor Kay

innovative in their responses to privacy concerns.[40] As evidence, he points to the fact that "state law preceded federal law in granting identity theft victims a right to free copies of their credit reports."[41] Third, and finally, by virtue of the prior two impacts, states have acted as laboratories for "simultaneous experiments with different policies."[42] This refrain has long figured in U.S. discussions of federalism, and not just in the context of privacy concerns.[43]

2. The United States Should Work Toward Developing More and Better Sectoral Privacy

Paul Schwartz's discussion of states' impacts on advancing and bettering privacy regulation includes an argument against adoption of an omnibus federal privacy bill, which would likely preempt more tailored state law and reduce sectoral experimentation at the federal level.[44] We tend to disagree.[45] But it is beyond the scope of this paper to evaluate, let alone compare, the relative merits of a sectoral

---

Lively, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Aug. 11, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/AD4M-X8B7].

40. Schwartz, *supra* note 21, at 917.

41. *Id.*

42. *Id.* at 918.

43. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("To stay experimentation in things social and economic is a grave responsibility. Denial of the right to experiment may be fraught with serious consequences to the nation. It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

44. Schwartz, s*upra* note 21, at 902 (arguing that "it would be a mistake for the United States to enact a comprehensive or omnibus federal privacy law for the private sector that preempts sectoral privacy law").

45. We are not alone in this belief. Bill Gates has called for enactment of a comprehensive federal privacy bill. Grant Gross, *Microsoft's Bill Gates Wants New Privacy Law*, CIO (Mar. 7, 2007), https://www.cio.com/article/266989/security-privacy-microsoft-s-bill-gates-wants-new-privacy-law.html [https://perma.cc/W3E8-F3A8]. So too, at various times, have corporations like Google, eBay, Intel, Hewlett-Packard, and Oracle. Erika Morphy, *Tech Giants Form Consumer Privacy Rights Forum*, TECHNEWSWORLD (Jun. 21, 2006), http://www.technewsworld.com/story/51272.html [https://perma.cc/B7T5-LTWB]. As noted by Paul Schwartz, proponents of unified federal privacy regulation argue that such an approach would "harmonize the U.S. regulatory approach with that of the European Union (EU), and possibly minimize international regulatory conflicts about privacy." Schwartz, *supra* note 21, at 904. In fact, at least one author has advocated not simply for omnibus federal privacy legislation, like the GDPR, but for establishment of a federal privacy agency, perhaps called the Privacy Protection Board. Gellman, *supra* note 17, at 1207. This proposal pushes the agency as a nonregulatory body, similar to the Civil Rights Commission that Congress established in the Civil Rights Act of 1957. *Id.* at 1197–99. Despite a lack of enforcement power, the proposal urges that the Commission still had key features that make it an appropriate parallel for the potential Privacy Protection Board: "independence, fact-finding functions, limited powers, and the highly controversial subject of its mandate." *Id.* at 1197. Robert Gellman notes that, with the power to assemble documented information and incorporate same into the public record, the Privacy Protection Board would be able to build an unimpeachable factual record of the status of privacy protection throughout the country. *Id.* at 1197–98. It would then use that foundation to advocate new and better privacy policies.

versus an omnibus approach. Our more modest claim here is not that a sectoral approach is necessarily superior to an omnibus privacy law, but rather that, even if one is limited to a sectoral strategy by political constraints, we still can achieve far more than the relevant agencies have yet attempted. Ironically, we are in some sense arguing against our preferences, because if we are right about the untapped power of the sectoral approach, then we are in effect strengthening Schwartz's argument for it as expressed in *Preemption and Privacy*.[46]

We can do more sectorally, and we can do it now. The first step to achieving progress, even in the arguably second-best world of sectoral regulation, is to understand what is possible. Thus, the main argument of this Article is that agencies with a safety mission already have the regulatory authority they need to make significant privacy-protective rules. In other words, the United States' extant sectoral approach to privacy governance has much more potential for privacy-enhancing regulation than has previously been recognized, and agencies should therefore take advantage of this authority.

II. WHAT SELECTED AGENCIES CAN DO TO PROTECT PRIVACY

A. How Administrative Agencies Interpret and Exercise Their Authority—And How Courts Review Them

In each of the next six sections of this Part, we set out a series of proposals for how an existing U.S. federal agency can use its regulatory authority, derived from existing statutes, to make pro-privacy rules. In most cases, this would require that the agency make at least a small change or expansion to its current understanding of its mandate. Due to recent Supreme Court decisions, that has suddenly become a slightly fraught endeavor, and it, therefore, pays to take a brief detour into the current and rapidly evolving law about what deference courts owe to an agency's interpretation of its governing law.

Agencies derive their authority to issue regulations from statutes. Although some statutes are detailed, many give an agency broad authority to address an issue by "filling in the details"[47] about how to solve a problem that Congress has identified. Agencies, at least in the progressive vision of government that has dominated since the New Deal, allow Congress to harness specialized expertise in service of congressional goals. Also, agencies can react more nimbly to changes in knowledge or circumstances than might be possible if Congress continually had to amend a statute to permit an agency to tackle new aspects of a problem or to update its approach to an old one.

When Congress delegates a broad-brush task to an agency, such as prohibiting unfair practices in commerce[48] or providing for the safety and effectiveness of medical devices,[49] it is first up to the agency to decide how far its authority extends and what to do with that authority. Decisions to regulate necessarily have at least two parts. One is a policy question in which the agency

---

46. *See* Schwartz, *supra* note 21, at 902.

47. Felix Frankfurter, *The Task of Administrative Law*, 75 U. PA. L. REV. 614, 614 (1927) (calling the phrase a euphemism for what amounts to law-making authority).

48. *See infra* Section II.B (FTC).

49. *See infra* Section II.D (FDA).

must decide whether a given problem merits the agency's attention and commitment of resources. This is important because even so-called informal rulemaking can be lengthy and expensive. Agencies must build a factual record, issue a notice of proposed rulemaking for public comments, digest the comments, and issue a final rule combined with a preamble in which the agency gives its reasons and replies to—whether or not it adopts—comments from the public. The second part is a legal question: whether the agency's governing statutes give it the authority to regulate private activity to solve, or at least ameliorate, a problem in a meaningful way. As a logical matter, the legal question might appear to precede the policy question, but sometimes an agency first finds itself confronted with a new problem and then must decide whether and how its authority may empower it to meet the needs of the moment. Conversely, if an agency takes an overly cramped view of the extent of its authority, it may ignore policy options that it might have selected if it properly understood its legal powers.[50]

Since 1984, the Supreme Court's guidance to lower courts[51] about how to review agencies' interpretations of their statutory authority has revolved around the so-called *Chevron* doctrine.[52] As regards informal "notice-and-comment" rulemaking,[53] *Chevron* famously tells courts to use a two-step method to review an agency's interpretation of its enabling statutes:[54]

> When a court reviews an agency's construction of the statute which it administers, it is confronted with two questions. First, always, is the question whether Congress has directly spoken to the precise question at issue. If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress. If, however, the court determines Congress has not directly addressed the precise question at issue, the court does not simply impose its own construction on the statute, as would be necessary in the absence of an administrative interpretation. Rather, if the statute is silent or ambiguous with

---

50. *Cf.* SEC v. Chenery Corp., 318 U.S. 80, 94–95 (1943) [hereinafter Chenery I] (holding that courts correcting an agency's understanding of governing law must remand to agency to allow it to make unconstrained policy choice on correct legal basis).

51. Scholars have noted that the Supreme Court itself does not appear to follow its own *Chevron* doctrine with great fidelity. *See* Michael Herz, Chevron *Is Dead: Long Live* Chevron, 115 COLUM. L. REV. 1867, 1870 n.20 (2015) (collecting sources). It may be that lower courts are not following *Chevron* reliably either. *See* Bethany Ring, Chevron *Deference: An Empirical Review of Rigor of Application at the District Court Level*, 24 CHAP. L. REV. 613, 632 (2021).

52. Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984).

53. Additional steps apply to less-than-formal rulemaking, *see, e.g.*, United States v. Mead Corp., 533 U.S. 218 (2001), or in informal adjudications, *id*., where there are reasons to believe that Congress did not give the agency "authority to determine the particular matter at issue in the particular manner adopted." City of Arlington v. FCC, 569 U.S. 290, 306 (2013).

54. Importantly, *Chevron* does not apply to any statute other than those where the agency is presumed to have unique expertise and Congress intended the agency's decision to have force of law because in those statutes there is no indication that Congress intended such a ruling to carry the force of law. *Mead Corp.*, 533 U.S. at 221.

> respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute.[55]

Thus, under *Chevron*, courts should strike down an agency's statutory interpretation of its powers under "step one" only if the statute unambiguously forecloses the agency's view; courts can also uphold an agency's interpretation as unambiguously correct. If, however, the statute is sufficiently ambiguous, then under "step two," courts are to uphold the agency's interpretation so long as it is "based on a permissible construction of the statute"—the interpretation must be reasonable, but not necessarily optimal. *Chevron* is rooted in a theory of congressional intent in which Congress intends that ambiguities in an agency-administered statute "be resolved, first and foremost, by the agency . . . rather than the courts."[56] Further, in 2013, in *City of Arlington, Texas v. FCC*,[57] the Supreme Court resolved a debate over the breadth of *Chevron* deference and held that *Chevron* deference applies not just to ordinary statutory interpretation but to "interpretation of a statutory ambiguity that concerns the scope of its regulatory authority (that is, its jurisdiction)."[58]

Chevron applies with equal force when an agency discovers a power in a statute that it had not formerly asserted, but there is an exception to *Chevron* deference when an agency issues a rule on a "major question." In *Food & Drug Administration v. Brown & Williamson Tobacco Corp.*, the FDA had asserted a power to regulate tobacco, a power it had long denied having. In deciding that the FDA lacked this power, the Supreme Court relied on, or perhaps gave birth to,[59] the "major questions doctrine," stating that "*Chevron* deference is premised on the theory that a statute's ambiguity constitutes an implicit delegation from Congress to the agency to fill in the statutory gaps," but "[i]n extraordinary cases, . . . there may be reason to hesitate before concluding that Congress has intended such an implicit delegation."[60]

Since deciding *Brown & Williamson* in 2000, the Supreme Court has invoked the "major questions" doctrine six more times. In *Gonzales v. Oregon*, the Court relied on the doctrine to strike down an interpretative rule preventing physicians from prescribing controlled substances for physician-assisted suicide under Oregon's Death with Dignity Act.[61] In *Utility Air*, the Court rested its decision on the economic consequences of the EPA's new assertion of a power to regulate thousands of greenhouse gas emitters.[62] The Court found the agency's assertion

---

55. *Chevron*, 467 U.S. at 842–43 (1984) (footnotes omitted).

56. *City of Arlington*, 569 U.S. at 296 (citing Smiley v. Citibank (South Dakota), N. A., 517 U.S. 735, 740–41 (1996)).

57. 569 U.S. 290 (2013).

58. *Id.* at 293.

59. *See* Natasha Brunstein & Richard L. Revesz, *Mangling the Major Questions Doctrine*, 74 ADMIN. L. REV. 217, 218 (2022). One could say that the idea actually dates back to a 1994 decision on telephone regulation. *See id.* at 324 (citing MCI Telecommunications Corp. v. AT&T, 512 U.S. 218 (1994)).

60. FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 159 (2000).

61. Gonzales v. Oregon, 546 U.S. 243 (2006).

62. Util. Air Regul. Grp. v. EPA, 573 U.S. 302, 323–24 (2014).

"unreasonable because it would bring about an enormous and transformative expansion in EPA's regulatory authority without clear congressional authorization."[63] Notably, Justice Scalia's opinion for the Court also stated that "[w]hen an agency claims to discover in a long-extant statute an unheralded power to regulate 'a significant portion of the American economy,' [citing *Brown & Wilkinson*], we typically greet its announcement with a measure of skepticism."[64]

Then, the Supreme Court relied on the "major questions" doctrine to deny *Chevron* deference to the IRS's interpretation of the Patient Protection and Affordable Care Act ("ACA"), labeling it an "extraordinary case[]" where "there may be reason to hesitate before concluding that Congress has intended such an implicit delegation" of authority to make the rule.[65] Chief Justice Roberts also noted that it was "unlikely that Congress would have delegated this decision to the IRS, which has no expertise in crafting health insurance policy of this sort."[66]

The Court returned to the "major questions" doctrine three times during the October 2021 term. First, in *Alabama Association of Realtors*, the Supreme Court held that the nationwide eviction moratorium for residential rental properties imposed by the Director of Centers for Disease Control and Prevention ("CDC") was plainly not authorized by statute[67]—a *Chevron* step-one problem, it would seem. But the Court added that "[e]ven if the text were ambiguous, the sheer scope of the CDC's claimed authority under § 361(a) would counsel against the Government's interpretation. We expect Congress to speak clearly when authorizing an agency to exercise powers of vast economic and political significance."[68]

A similar clear-statement requirement appeared when the Court upheld a preliminary injunction against OSHA's plan to require COVID vaccination or testing. Although the per curiam opinion did not use the words "major question," it did reiterate a clear-statement rule that likely amounts to much the same thing, saying that the OSHA rule was

> a significant encroachment into the lives—and health—of a vast number of employees. "We expect Congress to speak clearly when authorizing an agency to exercise powers of vast economic and political significance." Alabama Assn. of Realtors v. Department of Health and Human Servs., 594 U. S. ___, ___ (2021) (per curiam) (slip op., at 6) (internal quotation marks omitted). There can be little doubt that OSHA's mandate qualifies as an exercise of such authority.[69]

---

63. *Id.* at 324.
64. *Id.*
65. King v. Burwell, 576 U.S. 473, 485 (2015).
66. *Id.* at 486.
67. Ala. Ass'n of Realtors v. Dep't of Health & Hum. Servs., 141 S. Ct. 2485 (2021).
68. *Id.* at 2489 (cleaned up).
69. Nat'l Fed'n of Indep. Bus. v. Dep't of Lab., Occupational Safety and Health Admin., 142 S. Ct. 661, 665 (2022) (per curiam) (slip op. Jan 13, 2022).

Meanwhile, Justice Gorsuch's concurrence relied almost entirely on the OSHA rule being a "major question"—in those words.[70]

Third, and potentially most sweepingly, the Supreme Court relied on the "major questions" doctrine to decide *West Virginia v. EPA*.[71] Chief Justice Roberts wrote for six Justices, of whom two also joined in a more aggressive concurrence. On its face, the Chief Justice's opinion is hard to parse. First, he said the case was not moot even though the Clean Power Plan regulation at issue had been withdrawn.[72] Then, he asked whether Congress could have intended the agency's construction of the statute, working through the lens that in "certain extraordinary cases, both separation of powers principles and a practical understanding of the legislative intent make us 'reluctant to read into ambiguous statutory text' the delegation claimed to be lurking there."[73] The majority then says the statute fails the test.[74]

This holding suggests an anti-*Chevron* interpretive canon: in "extraordinary" cases, when a matter is a "major question," then ambiguity in the statute will constrain the agency; if it is not a "major question," then, under *Chevron* step two, the agency's resolution of the statutory ambiguity carries the day. *West Virginia v. EPA* suggests that the "major questions" doctrine has morphed into a new form of the nondelegation doctrine, one aimed at any delegation of regulatory duties that the Court is prepared to deem insufficiently specific. As a formal matter, by framing the rule as one that applies only to very big issues, the Court leaves *Chevron*'s two-step approach as the rule for ordinary regulations[75]—at least for the time being.

The Court's new majority appears to have no intention of giving *Chevron* deference to large exercises of regulatory power that the majority is willing to interpret as lacking the clearest statutory authorization, including those based on an agency's reinterpretations of its statutory authority.[76] What is not clear, however, is just how big an issue must be to be "extraordinary" enough to qualify for the "major questions" exception to *Chevron*.

In *West Virginia v. EPA*, the majority suggests that the "major questions" doctrine was an issue because of the EPA's attempt to assert "'unprecedented power over American industry.'"[77] And once the "major questions" doctrine was invoked, the Clean Power Program foundered due to the plan's novelty, as well as what the

---

70. *See id.* at 669 (Gorsuch, J., concurring).

71. West Virginia v. EPA, 142 S.Ct. 2587, 2610 (U.S. June 30, 2022).

72. *Id.* at 2607.

73. *Id.* at 2609 (quoting Util. Air Regul. Grp. v. EPA, 573 U.S. 302, 324 (2014)).

74. Justice Kagan's dissenting opinion, *see id.* at 2626 (Kagan, J., dissenting), persuasively demonstrated that the statute not only was clear and not ambiguous but that it permitted precisely what the Clean Power Plan would have involved.

75. *Cf.* Aaron L. Nielson, *The Minor Questions Doctrine*, 169 U. PA. L. REV. 1181, 1193–94 (2021).

76. *See* Lisa Heinzerling, *The Power Canons*, 58 WM. & MARY L. REV 1933 (2017).

77. *West Virginia*, 142 S. Ct. at 2612 (quoting Indus. Union Dep't, AFL-CIO v. Am. Petroleum Inst., 448 U.S. 607, 645 (1980) (plurality opinion)).

majority somewhat dubiously characterized as the EPA's reinterpretation of its statutory powers to allow the agency to assert a regulatory power not clearly visible from the text of the statute. As Daniel Deacon and Leah Litman put it, "[t]he novelty of an agency's regulatory approach is an indication that the policy is major and therefore likely not authorized by statute."[78] Any "unprecedented" assertion of authority thus becomes a potential target of more searching review.[79] These elements of the "major questions" doctrine have implications for an argument, such as ours, that agencies should (re)interpret their safety missions to include privacy. According to Chief Justice Roberts, the very fact that the agency has not previously asserted a power raises a question as to "'whether such [a] power was actually conferred'."[80]

Nevertheless, as a doctrinal matter, we do not think anything we propose is likely to rise to the "extraordinary" level required to trigger application of the "major questions" doctrine. Either the agency's interpretation is clearly within its statutory delegation, or—even if it that is ambiguous—the economic consequences will not rise near the level of the challenged regulations in the cases where the Court has so far invoked the doctrine. Ironically, the very fact often lamented by privacy scholars, that privacy harms are so often hard to monetize,[81] will work in favor of those arguing for the viability of understanding an agency's safety mission to include privacy. In addition, cautious agencies can minimize their risk of being reversed in court by starting with data privacy requirements that have substantial benefits to consumers but do not plausibly impose large financial costs on a wide swath of firms.

On the other hand, the majority's appeal, however cursory, to a form of post-enactment legislative history is more troubling, both for our proposal and for the future of regulation more generally. The opinion states, "we cannot ignore that the regulatory writ EPA newly uncovered conveniently enabled it to enact a program that, long after the dangers posed by greenhouse gas emissions 'had become well known, Congress considered and rejected.'"[82]

The two general problems with this argument should be obvious. First, by suggesting that congressional inaction might have legal weight, the Court violates the *Chadha* principle that, barring a few textual and historical exceptions, Congress cannot create legal consequences for anyone outside the legislative branch without

---

78. Daniel Deacon & Leah Litman, *The New Major Questions Doctrine*, 109 VA. L. REV. (forthcoming 2022) (manuscript at 49), https://ssrn.com/abstract=4165724.

79. *Id.* at 49–50.

80. *West Virginia*, 142 S. Ct. at 2610 (quoting FTC v. Bunte Bros., Inc., 312 U.S. 349, 352 (1941).

81. In *Doe v. Cao*, 540 U.S. 614, 616 (2004) the Supreme Court held that there was no standing to claim statutory damages without "actual" damages. *FAA v. Cooper*, 566 U.S. 284, 287 (2012), held that emotional distress alone was insufficient to clear the "actual" damages bar. And then *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016), turned the harm requirement into a standing bar for private rights of actions seeking damages for privacy harms. For a discussion of how this came to be and how better to understand privacy harms, see Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. REV. 793 (2022).

82. *West Virginia*, 142 S. Ct. at 2614 (quoting FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 144 (2000)).

bicameralism and presentment.[83] Inaction, by definition, lacks at least presentment. Second, it is the rare remedial statute that sails through Congress on its first attempt. Today, with the filibuster and entrenched partisan gridlock, it is the rare bill that gets through Congress at all. If one took this rejected-proposal theory seriously, it could mean that agencies in general are now barred from trying anything new.[84] (Perhaps that is, in fact, where the "major questions" doctrine is heading.) And, certainly, new privacy-protective proposals would be off the table as Congress has never passed a comprehensive, national data-privacy rule, even if it has occasionally passed sectoral rules.[85]

When it comes to the Supreme Court, doctrine is not everything. In part because of the growth of the "major questions" doctrine, and in part due to changes in the composition of the Supreme Court, many commentators have suggested that even if the administrative state survives, *Chevron*'s days may be numbered.[86] Speculation as to what would follow varies. Perhaps the Court will return to pre-*Chevron* methods of statutory interpretation, under which the Court itself always decided the correct interpretation of a statute, but agencies' views were sometimes treated as persuasive authority.[87] Or, perhaps the Court will take a new antiregulatory path and only approve of regulations, large or small, that were clearly and unambiguously foreseen by the enabling statute, thus enacting a near-total brake on the administrative state that the *Lochner*-era Court could only have dreamed of.

If that sweeping shift occurs, the arguments about agency authority that follow may join many others in the storage locker of history. Until that day, however, any proposal that depends on persuading agencies to reinterpret their statutory authority more broadly must recognize the need for that authority to be textually plausible, and for the economic consequences to be smaller than the consequences were to the tobacco industry in *Brown & Wilkinson*, to the automobile makers and small factories in *Utility Air*, and to the firms (and even though not direct

---

83. *See* Immigr. & Naturalization Serv. v. Chadha, 462 U.S. 919, 954–55 (1983).

84. This would be consistent with the Court's recent decisions in its appointment-and-removals jurisprudence that have severely limited Congress's attempts to experiment with varying types of structures for federal agencies. *See* Deacon & Litman*, supra* note 78, at 38.

85. *E.g.*, Genetic Information Nondiscrimination Act of 2008, 29 U.S.C. §§ 216–1191(b), 42 U.S.C. §§ 300–1395; Financial Services Modernization Act of 1999, 12 U.S.C. §§ 24(a)–2908, 15 U.S.C. §§ 8(b)–6827 (the Gramm-Leach-Bliley Act); Health Insurance Portability and Accountability Act of 1996, 18 U.S.C. §§ 24–3486, 26 U.S.C. §§ 220–6039(F), 29 U.S.C. §§ 1181–1191(c), 42 U.S.C. §§ 300–1320(d)(8) [hereinafter HIPAA]. Were the rejected proposal doctrine to prove more than a makeweight, one can only imagine what a future Supreme Court might say if Congress fails to pass the American Data Privacy and Protection Act. *See infra* text accompanying notes 232–37.

86. *See generally, e.g.*, Ronald M. Levin, *The APA and the Assault on Deference*, 106 MINN. L. REV. 125 (2021); Kristin E. Hickman & Aaron L. Nielson, *The Future of* Chevron *Deference*, 70 DUKE L.J. 1015 (2021); Kristin E. Hickman, Aaron L. Nielson, *Narrowing* Chevron*'s Domain*, 70 DUKE L.J. 931 (2021); Cass R. Sunstein, *Zombie* Chevron*: A Celebration*, 82 OHIO ST. L.J. 565 (2021); Lisa Schultz Bressman & Kevin M. Stack, Chevron *Is a Phoenix*, 74 VAND. L. REV. 465 (2021) (arguing that even if the Supreme Court kills the *Chevron* doctrine, it will rise again).

87. *See* Skidmore v. Swift & Co., 323 U.S. 134, 140 (1944).

parties, workers) in *NFIB v. OSHA*. To the still-large extent that *Chevron* continues to control the judicial review of ordinary agency rulemaking, the rules and underlying interpretations we propose below are sufficiently narrow to be less-than-major questions. Consequently, any challenge to them should be evaluated under the *Chevron* framework: first, did Congress speak directly to the issue, and second, if not, are the proposed reinterpretations we offer reasonable readings of the statutes?

Privacy as Safety[88] offered an argument for why privacy ought to be considered an integral component of safety, or at least a substantial contributor to it.[89] For four of the agencies discussed below, the FDA,[90] NHTSA,[91] the FAA,[92] and—yes—OSHA,[93] their statute charges the agency with protecting individual "safety" of some kind. In those cases, we believe that so long as no "major question" is involved, all the agency will need to do is adopt an expanded understanding of what "safety" means, and this redefinition probably should prevail under ordinary statutory construction or receive step-one *Chevron* deference, and failing that, certainly should succeed under *Chevron* step two.[94]

Two of the agencies discussed below, the FTC and the CPSC, have somewhat differently expressed authority. The FTC is charged with prohibiting unfair trade practices[95]—and a firm's spying on its customers or selling information

88. Froomkin & Colangelo, *supra* note 1.

89. The argument is summarized *supra* Section I.A.

90. The Federal Food, Drug, and Cosmetic Act is designed "to provide for the safety and effectiveness of medical devices intended for human use." *See infra* Section II.D.

91. In the National Traffic and Motor Vehicle Safety Act of 1966 (Safety Act of 1966), Congress "determine[d] that it [was] necessary to establish motor vehicle safety standards for motor vehicles and equipment . . . ." *See infra* Section II.E. The Act directed the Secretary of Transportation to promulgate "Federal motor vehicle safety standards," defined as "minimum standard[s] for motor vehicle performance, or motor vehicle equipment performance, which [are] practicable, which meet[] the need for motor vehicle safety and which provide[] objective criteria." *See id.*

92. The FAA inherited authority under the Civil Aeronautics Act to "promote the development and safety . . . of civil aeronautics." *See infra* Section II.F. In a declaration of policy, Congress noted that the CAA's regulation of aircraft should seek to "assure the highest degree of safety in" air travel. *See id.*

93. The Occupational Safety and Health Act of 1970 directs OSHA to "assure so far as possible every working man and woman in the Nation safe and healthful working conditions." *See infra* Section II.G.

94. We do not think the term "safety" is even arguably vague. It is a common term, and it should not be surprising to anyone that new dangers can arise over time and that agencies charged with ensuring "safety" would therefore have the authority to react to new potential sources of harm. Note that in the case of the FTC, "Congress affirmatively made a decision" in both the original FTC Act in 1914 and in the 1938 amendments expanding the FTC's authority to include policing commerce for deception and unfairness "to choose vague language" in order to allow the agency to adapt to new problems as they arose. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 119–20 (2016).

95. *See infra* Section II.B. Similarly, the Consumer Financial Protection Bureau (CFPB) is charged with policing unfairness in consumer financial services. *See* 12 U.S.C. §§ 5531, 5536(a). The CFPB recently relied on this authority to issue guidance stating that entities under its jurisdiction that fail to have adequate data protection or information security

about what goes on in the consumers' homes would, we submit, amply fall within that ambit. Indeed, FTC precedent suggests that the agency has the power to punish firms for their failure to disclose dangers to consumers.[96] Separately, the FTC has authority to issue rules defining what constitutes an unfair or deceptive practice in commerce.[97]

Congress gave the CPSC the power to protect the public "against unreasonable risks of injury associated with consumer products."[98] As we will show, it takes relatively little effort to see potential privacy injuries as falling within this existing authority.

A more difficult question is whether any of the statutory reinterpretations we propose below, and the regulations that we suggest are enabled by them, could plausibly be called a "major question." The question is doubly difficult because the Supreme Court has offered so little guidance as to what is major—the line drawn by the precedents to date is at best amorphous, and because until actual rules are written it may in some cases be difficult to say how "major" the proposed rules would be. We do not see any of our proposals as threatening to put an industry out of business, so they are much less significant than those in *Brown & Wilkinson*; some rules would benefit a very large class of people, but each in small ways, distinguishing them from *Alabama Association of Realtors*, *Utility Air,* and—depending on how one rates the nature of the imposition—*NFIB v. OSHA*.

Armed with this background regarding an agency's flexibility to reinterpret its statutory powers, we turn now to individual examinations of six agencies that could, if they chose, find substantial authority to make privacy-protecting rules relating to their regulatory domains.

B. The Federal Trade Commission (FTC)

In the absence of a true U.S. Privacy Commission, the FTC is arguably the United States' leading federal privacy regulator—but here the agency is surmounting a low bar. The FTC has the authority, if it chooses to exercise it, to do substantially more to protect privacy than it currently does.

The FTC may be the de facto federal privacy regulatory body in the United States,[99] but at present most of the FTC's efforts consist of enforcement actions

---

for customer data are acting unfairly and thus subject to sanctions even in the absence of actual injury to consumers. *See* Consumer Financial Protection Circular 2022-04: Insufficient Data Protection or Security for Sensitive Consumer Information, 87 FED. REG. 54346–49 (Sept. 6, 2022).

96. *See infra* Section II.B.1.

97. *See infra* Sections II.B.1.a, b.

98. *See infra* Section II.G.

99. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598 (2014); Ian M. Davis, *Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads*, 69 EMORY L.J. 781, 789 (2020) (discussing how "the Federal Trade Commission has emerged as the 'de facto' data protection authority" in the United States).

rather than rulemaking.[100] Currently, "[t]he FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take steps to remediate the unlawful behavior."[101] The FTC has used its authority to bring "hundreds of privacy and data security cases to date."[102] In a prominent example, the FTC brought a privacy-related enforcement action against Facebook that led to a $5 billion fine, "the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide."[103] In addition to the sizeable fine, Facebook agreed to "submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users' privacy."[104] Highly visible enforcement actions arguably have a broad impact on privacy practices,[105] and certainly have had an impact on written privacy policies, but *ex ante* rules directed at privacy protection would have a much broader effect.[106]

Although Congress is currently considering privacy legislation,[107] we believe the FTC could do much more without waiting for additional regulatory authority.

1. Invoking the FTC's Enforcement Authority When Firms Fail to Disclose Privacy Risks

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[108] Since the early 1980s, the FTC has interpreted its authority to regulate "unfair or deceptive" acts or practices as reaching any material "representation, omission or practice that is likely to mislead the consumer acting

---

100. FTC, PRIVACY & DATA SECURITY UPDATE: 2019 1 (2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf [https://perma.cc/B45M-4GBN] [hereinafter FTC 2019 UPDATE].

101. *Id.*

102. *Id.*

103. FTC, Press Release, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/HC4N-UF8S].

104. *Id.*

105. *See* Solove & Hartzog, *supra* note 99, at 598 (discussing how "many privacy lawyers and companies view the FTC as a formidable enforcement power, and they closely scrutinize FTC actions in order to guide their decisions").

106. Davis, *supra* note 99, 814–16 (arguing that, "[w]hile ad hoc adjudication and settlement were appropriate during the FTC's initial foray into data security, the landscape has changed" and a rulemaking process would "provide the FTC with (1) a democratically constructed and higher quality data security standard; (2) a more efficient use of administrative resources; and (3) a remedial capacity better suited to protecting consumers").

107. *See* American Data Privacy and Protection Act, H.R. 8152, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf [https://perma.cc/W24X-7ZLG]. *See also infra* text accompanying notes 232–37.

108. 15 U.S.C. §§ 45(a)(1), 52(b).

reasonably in the circumstances, to the consumer's detriment,"[109] or any practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[110] Thus, in its enforcement of § 5, the FTC has two bases for finding privacy violations—"deceptive" trade practices and "unfair" trade practices.[111]

a. Deception

Since 1983, the FTC has pursued a policy designed to protect consumers from deceptive advertising. Under the FTC's "Deception Policy,"[112] the agency prohibits a representation, omission, or practice as deceptive if it "is likely to mislead consumers acting reasonably under the circumstances and is material to consumers."[113]

For the FTC to find deception, it must find three things: First, the FTC must find that "a representation, omission, or practice occurred";[114] these are typically "written or oral misrepresentations, or omissions of material information."[115] Second, the FTC must find that the deceptive act or practice was "likely to mislead reasonable consumers under the circumstances."[116] Under this prong, the FTC "considers the totality of the practice in determining how reasonable consumers are likely to respond."[117] Third, the FTC must find that the statement or omission was "a material one": that is, a statement or omission regarding "information that is important to consumers."[118] Notably, the FTC "considers claims or omissions material if they significantly involve health, safety, or other areas with which the reasonable consumer would be concerned."[119]

In other words, the FTC requires firms to make honest disclosures if consumers' buying decisions or, critically, consumers' conduct regarding a product

---

109. *See* FTC Letter from James C. Miller III to Hon. John D. Dingell (Oct. 14, 1983), 103 F.T.C. 174, 175 (1984) (appended to Cliffdale Assocs., Inc., 103 F.T.C. 110 (1984)) [hereinafter FTC Statement on Deception]; *see also* HOOFNAGLE, *supra* note 94, at 123–25; Solove & Hartzog, *supra* note 99, at 599.

110. 15 U.S.C. § 45(n).

111. Both bases can serve as justifications for a single enforcement action.

112. FTC Statement on Deception, *supra* note 109, at 175.

113. *Id.* at 176. The FTC announced the original policy in a letter, leading some to question if it was a true policy statement. *See* Comment, Dale Pollack & Bruce Teichner, *The Federal Trade Commission's Deception Enforcement Policy*, 35 DEPAUL L. REV. 125, 126 (1985). But in fact, the FTC officially adopted the Deception Policy in a 3–2 vote. HOOFNAGLE, *supra* note 94, at 123.

114. FTC Statement on Deception, *supra* note 109, at 176.

115. *Id.*

116. *Id.* at 177.

117. *Id.* at 178.

118. *Id.* at 182.

119. *Id.*

or service would likely be materially altered by a firm's false representation, its accurate but potentially misleading representation,[120] or its omission.

The idea that a material omission is as troubling as an overtly false statement appears in the 1983 Statement on Deception. The FTC relied on this idea alone to decide the 1984 action *In re International Harvester Co.*; there, the FTC held that a failure to notify consumers about hidden hazards in a product (in this case, occasional "fuel geysering" in farm tractors) constituted deception.[121] However, the FTC does require that failures to disclose be material.[122]

The FTC began focusing on privacy issues in 1995,[123] and its initial privacy-related enforcement actions relied on the deception rationale.[124] By then, however, the idea that the antideception duty included a duty to disclose hazards was well established. Then, as today, the FTC considered it deceptive to sell "hazardous . . . products or services without adequate disclosures."[125] Indeed, the FTC now has a considerable track record of sanctioning firms that collect user data without notice, or with inadequate notice.[126] If privacy is a form of safety, and the absence of privacy can be a hazard, then it follows that misleading consumers about privacy hazards or failing to disclose privacy hazards is a form of deception that can trigger FTC enforcement if the deception could materially harm consumers.

b. Unfairness

The FTC's unfairness jurisdiction arises from its authority to regulate "unfair trade practices." To find a practice unfair, the FTC originally said in its 1980 Unfairness Statement that it must find that the practice (1) causes or is likely to cause substantial injury to consumers; (2) is not reasonably avoidable by consumers themselves; and (3) is not outweighed by countervailing benefits to consumers or to competition.[127] Notably, conduct that violates this three-part test need not violate any other statute to be sanctionable.[128] Congress codified, but modified, the FTC's 1980 Unfairness Statement in 1994,[129] effectively collapsing the three-part test into one: whether there is "unjustified consumer injury."[130]

---

120. *See* FTC Statement on Deception, *supra* note 109, at 159. Hoofnagle notes that the FTC originally adopted a reasonable person standard to evaluate this prong of the deception standard—and that "reasonable person" is a higher standard of proof than the FTC Act requires. HOOFNAGLE, *supra* note 94, at 125.

121. 104 F.T.C. 949, 1043 (1984).

122. HOOFNAGLE, *supra* note 94, at 126, 129–130.

123. Solove & Hartzog, *supra* note 99, at 598.

124. *Id.* at 599.

125. *See* FTC Statement on Deception, *supra* note 109, at 175.

126. For a survey of some leading enforcement actions, *see* Solove & Hartzog, *supra* note 99, at 631–36.

127. *See* Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators (Dec. 17, 1980) [hereinafter FTC Unfairness Policy Statement], reprinted in In re Int'l Harvester Co., 104 F.T.C. 949, 1073–74 (1984), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [https://perma.cc/R7BW-ZCP7].

128. *See* FTC v. Accusearch, 570 F.2d 1187, 1194 (10th Cir. 2009).

129. 15 U.S.C. § 45(n).

130. HOOFNAGLE, *supra* note 94, at 131.

Although the FTC has tended to rely more on a deception rationale, its use of unfairness claims has been growing since 2003, when it first relied on unfairness as an independent theory for privacy violations.[131] As a general matter, the FTC now treats the practice of making products look safer than they are as a form of unfairness as well as deception.[132] And, notably, the FTC treats the collection of personal information, when done without notice or in any other deceitful way, as an unfair act.[133]

The agency has not hesitated to label surveillance and other privacy harms as unfair practices. In 2003, the FTC brought an early unfairness prosecution relating to personal information against a firm that was secretly recording consumers in the home, without alleging monetized damages.[134] Similarly, in a quiet echo of the GDPR, several FTC enforcement actions have also treated the improper use of data that was not necessarily collected improperly as an unfair practice.[135] Both of these are potentially significant constraints on privacy-harming commercial behavior.

c. Limits to FTC Enforcement Powers

Unfortunately, the FTC's privacy enforcement powers have significant limits. As noted above, the FTC can act if a firm makes privacy promises it does not keep because that is deception.[136] Similarly, the FTC can act under the omission prong of its deception authority if a firm fails to disclose an important aspect of how it collects or uses data. And the FTC can use its unfairness authority to sanction improper uses of even legitimately collected data (and probably more).

Nevertheless, it should be noted that even if the FTC does not necessarily require monetizable harms to sanction overt actions, the materiality element imposes limits on the FTC's ability, or willingness, to go after so-called pure omissions that have no other deceptive element. Today, both the agency and the courts will likely require evidence of an actual or at least plausible potential harm to consumers from the omission, and they will likely mistrust claims that can be characterized as

---

131. *Id.* at 161; Solove & Hartzog, *supra* note 99, at 638.

132. See, for example, the FTC's description of the sales pitch for the "Amazing Gut Buster" as both unfair and deceptive due to the failure, among other things, to disclose the "risk of injury to users from snapping or breakage of the product's spring or other parts." In re Consumer Direct, Inc., 111 F.T.C. 923, 925–26 (1990). We are indebted to Woody Hartzog for pointing us to this snappy example.

133. Solove & Hartzog, *supra* note 99, at 641–42 (citing enforcement actions and judicial decisions upholding them). The FTC has also suggested that in some cases the design of a product may itself be deceptive. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 142–46 (2018).

134. *See* In re DesignerWare, LLC., FTC File No. 1123151 (Apr. 15, 2013), https://www.ftc.gov/legal-library/browse/cases-proceedings/112-3151-designerware-llc-matter [https://perma.cc/A9SF-BCAM].

135. *See, e.g.*, Solove & Hartzog, *supra* note 99, at 642 (citing complaints in *In re Aspen Way Enterprises* and *FTC v. Hill*).

136. Indeed, in the early *Cliffdale Associates, Inc.* action, the Commission expressly dismissed an unfairness charge, distinguishing it from the deception charge that it upheld. 103 F.T.C. 110 (1984).

relating to extraneous matters.[137] Although it addressed Massachusetts's "Little FTC Act,"[138] the First Circuit's recent decision in *Tomasella v. Nestlé USA, Inc.*[139] may be instructive. There, the First Circuit held that Nestle's failure to disclose the child-labor policies of its cocoa bean suppliers was neither a deceptive act or practice nor an unfair one, under Massachusetts law, in part because the omission was too tangential to whether and how consumers used the product.[140] In addition, the failure to disclose the child-labor policies did not create a cognizable injury or loss to consumers because the harm was purely subjective.[141] For better or worse, at least since the enactment of § 45(n) in 1994, the FTC has not accepted a violation of an established public policy, without more, as triggering its unfairness enforcement authority.[142]

Furthermore, the FTC issues relatively few privacy-related enforcement actions per year,[143] and the actions that do arise usually conclude with consent decrees.[144] Initial fines are often small.[145] Repeat offenders, however, may incur substantial fines. Nevertheless, the overall effect of this enforcement regime geared to accurate disclosure is, at best, to produce accurate disclosure.

Disclosure is valuable. It may allow consumers, perhaps informed by expert intermediaries, to make better choices about the information practices of the firms with which they choose to transact. Or the fear of market blowback may constrain firms from doing things that they would rather not have consumers know about. There is, however, a competing narrative asserting that the main effect of an accurate-disclosure regime is that firms produce longer and truer privacy policies but do not change their potentially abusive information collection and usage practices. In this view, while consumers claim to be very concerned about privacy issues, they do not read what presents as pages of long, boring boilerplate, and firms suffer few or no consequences for disclosing injurious privacy policies.[146]

One of us has suggested that rational people may act this way because they suffer from "privacy myopia": they evaluate every datum about them at its (smaller)

---

137. The dueling concurrences in In re Lenovo, Inc., FTC File No. 1523134 (Sept. 5, 2017), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3134-lenovo-inc [https://perma.cc/8V5C-WZJF], showed there was some disagreement about even failures to disclose packaging of software that would make users' use of the internet less secure.

138. Specifically, MASS. GEN. LAWS ANN. ch. 93A, § 2.

139. 962 F.3d 60 (1st Cir. 2020).

140. *Id.* at 72–74.

141. Privacy harms can be hard to monetize, *see* Citron & Solove, *supra* note 81, at 793, but as argued in *Privacy as Safety*, Froomkin & Colangelo, *supra* note 1, collection and reuse of personal information can harm consumers in a more direct ways than the subjective, if undoubtedly real, unhappiness that may be caused when consumers discover they are buying unethically sourced products.

142. HOOFNAGLE, *supra* note 94, at 133.

143. Solove & Hartzog, *supra* note 99, at 600 (noting that, in 2014, the FTC was acting on about ten out of an average of 170 privacy-related complaints per year).

144. *See* HOOFNAGLE, *supra* note 94, at 159.

145. Solove & Hartzog, *supra* note 99, at 605.

146. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J.L. & POL'Y FOR INFO. SOC'Y 543, 565 (2008) (estimating that the average person would need 201 hours per year to read all the privacy policies they agreed to).

marginal value rather than its (larger) average value when data brokers and others aggregate the consumers' personal information into a single profile. As a result, there is a market failure in which consumers are overwilling, or under-cautious, about selling or exposing their personal data to firms and others.[147] If disclosure of privacy practices is not enough to cure this market failure, then something additional is needed. Indeed, as these consumer profiles become part of the Big Data required by predictive AIs, the need now may be greater than ever.[148] Fortunately, as we describe in the next section, the FTC has additional powers it can invoke to ban some privacy-harming practices, albeit at the cost of additional effort.

2. Invoking the FTC's Authority to Issue Regulations Protecting Consumer Privacy

There is a more difficult but also more powerful way the FTC could use existing statutory authority to protect consumer privacy. In § 202 of the FTC Act, Congress gave the FTC broad authority to issue rules defining unfair or deceptive practices prohibited by law.[149] Although Congress added significant procedural prerequisites to the FTC's authority to issue rules in its 1994 amendments to the FTC Act,[150] the FTC retains broad authority to define and proscribe unfair and deceptive commercial practices threatening consumer privacy, so long as the benefits of the regulation outweigh the costs.[151]

The issue of privacy rulemaking has been a political football. Although § 202 authority has been on the books since 1975,[152] the FTC has been shy about invoking it, and indeed, the FTC has yet to use this general rulemaking authority to protect consumer privacy interests.[153] One reason for the agency's hesitancy is

147. *See* A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1733–37; A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502–05 (2000) [hereinafter Froomkin, *Death of Privacy*].

148. *See* A. Michael Froomkin, *Big Data: Destroyer of Informed Consent*, 18 YALE J. HEALTH POL'Y. L. & ETHICS 27, 34–35 (2019), 21 YALE J.L. & TECH. 27, 34–35 (2019).

149. Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. 75-447 § 5(a) (1938); Pub. L. 93-637 § 202(a), 88 Stat. 2193, 2193–94 (1975) (codified as amended at 15 U.S.C. § 57a). For a discussion of the breadth of the FTC's unfairness authority as it relates to robots, see Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 810–13 (2015).

150. Federal Trade Commission Act Amendments of 1994, Pub. L. 103–312, 108 Stat. 1691, 1692 (1994) (codified at 15 U.S.C. § 57a); Davis, *supra* note 99, at 800–01.

151. Chris Jay Hoofnagle, Woody Hartzog, & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/Q5DM-BL4W]. *Cf.* Davis, *supra* note 99 (discussing how the FTC's "regulatory authority in the domain of data security appears well-settled").

152. *See* Hartzog, *supra* note 149, at 810–13.

153. The FTC has, however, issued rules directed at protecting privacy interests in specific contexts outlined by statute. Davis, *supra* note 99, at 813–21 (pointing out the FTC's experience formulating the GLBA Safeguard Rule, relating to financial institutions; the FACTA Red Flags Rule, relating to credit reporting; and the COPPA Rule, relating to the use of children's information as providing rulemaking experience in the privacy sphere).

surely that the so-called Magnuson-Moss procedure[154] requires more steps than ordinary notice-and-comment rulemaking,[155] although recent revisions to FTC procedures have streamlined the process somewhat.[156]

The FTC can invoke its power to make rules about unfair or deceptive business practices under the FTC Act "only where it has reason to believe that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent," and the FTC can find prevalence "only if—(A) it has issued cease and desist orders regarding such acts or practices, or (B) any other information available to the Commission indicates a widespread pattern of unfair or deceptive acts or practices."[157] "In addition, the FTC must provide advance notice of any proposed rulemaking to Congress, consider regulatory alternatives," "publish a 'statement of basis and purpose to accompany' the final [rule]," and "compile a 'rulemaking record' to be used in case of judicial review."[158]

a. The FTCs Anti-Deception Authority

The FTC's authority to ban deception is likely its most straightforward avenue to implementing privacy-related rules. Many threats to privacy arise from misleading or invisible-to-the-consumer acts or practices that therefore are deceptive, including but not limited to those discussed in the FTC's Statement on Deception.[159]

Moreover, as discussed above, threats to privacy often arise from omissions when a firm fails to warn consumers about privacy risks associated with its goods or services. The FTC could require as a general matter that firms disclose all but de minimis privacy risks on the grounds that a privacy-related omission would often be likely to mislead a reasonable consumer, given that consumers lack alternative sources of information regarding how a particular firm is using and protecting (or failing to protect) information. Lacking other sources of information, it is unlikely that a reasonable consumer would be able to identify an omission or a statement as misleading. Further, the agency could reasonably conclude that failing to disclose privacy risks would be material because, as *Privacy as Safety* argues, threats to privacy often threaten consumers' welfare.[160]

The FTC could also craft a rule defining as deception both the misstatement of a privacy risk and the failure to disclose a material privacy risk. A general rule of this nature would make enforcement simpler because, once the rule was in place, the

---

154. 15 U.S.C. §57a(b).

155. The IAPP published a useful infographic summarizing the multi-year process. *See* IAPP, *FTC Privacy Rulemaking: The Steps to Get There* (Dec. 2021), https://iapp.org/media/pdf/resource_center/ftc_privacy_rulemaking_infographic.pdf [https://perma.cc/77HJ-ZC9P].

156. *See* FTC, STATEMENT OF THE COMMISSION REGARDING THE ADOPTION OF REVISED SECTION 18 RULEMAKING PROCEDURES (July 9, 2021), https://www.ftc.gov/system/files/documents/public_statements/1591786/p210100commnstmtsec18rulesofpractice.pdf [https://perma.cc/GN5T-TR2Y].

157. 15 U.S.C. §57a(b).

158. Davis, *supra* note 99, at 800–01.

159. FTC Statement on Deception, *supra* note 109, at 175.

160. *See generally* Froomkin & Colangelo, *supra* note 1.

FTC would only need to prove the existence of the deception instead of also having to prove materiality and causation in every enforcement action.

In addition, the FTC could make a real difference in protecting consumer privacy by providing a blanket definition for common terms and saying that misusing those terms is per se deceptive. As discussed below, it could also label certain practices related to privacy policies as unfair. To make privacy policies more effective, the FTC could issue a rule defining a "standard set of meanings for key components [of privacy policies], such as access and correction rights, data collection, data sharing, [and] data security" and requiring firms to live up to these definitions if they include any of these terms in their privacy policies.[161] In addition to making privacy policies more uniform and protective, the FTC could also require companies to make them easily accessible. Drawing on its experience with disclosure requirements in advertisements,[162] the FTC could create requirements regarding how companies make consumers aware of their privacy policies.

In sum, the FTC can and should use its rulemaking authority under the deception prong to implement privacy protection.

b. The FTC's Anti-Unfairness Authority

The FTC originally interpreted unfairness to include almost any unsavory business practice.[163] The FTC's determination of whether something was unfair depended upon whether it "offend[ed] public policy"; "whether it [was] immoral, unethical, oppressive, or unscrupulous"; and "whether it cause[d] substantial injury to consumers (or competitors or other businessmen)."[164] The Supreme Court gave this position implicit support in 1972.[165]

In 1978, however, Congress showed its disapproval of the FTC's use of its broad unfairness authority after the FTC attempted to ban all advertisements directed at children.[166] Congress "refuse[d] to provide . . . necessary funding, and simply shut down the FTC for several days."[167] Congress also explicitly prohibited the FTC

---

161. Solove & Hartzog, *supra* note 99, at 674.

162. *Id.*; Hartzog, *supra* note 149, at 816 ("One of the most effective tools the FTC has is the power to regulate company disclosures in advertisements and other statements made in commerce.").

163. *See* J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection [https://perma.cc/HB9W-3KJ2] (citing FTC, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, Statement of Basis and Purpose, 28 Fed. Reg. 8355 (1964)).

164. Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, Statement of Basis and Purpose, 29 Fed. Reg. 8325, 8355 (1964).

165. *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239, 244 n.5 (1972) (citing the Cigarette Rule, *supra* note 164, as demonstrating an acceptable application of FTC unfairness authority).

166. *See* Beales, *supra* note 163.

167. *Id.*

from using its unfairness authority to regulate advertising to children.[168] To preserve its newly suspect unfairness authority, the FTC developed a narrower definition of unfairness.[169]

Outlined in an influential 1980 Policy Statement,[170] the FTC's narrower understanding of "unfairness" stated that "[t]o justify a finding of unfairness," the injury resulting from a practice "must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided."[171]

Through the FTC Act Amendments of 1994, Congress codified the FTC's narrow definition of "unfairness,"[172] but it also imposed additional limits on the FTC's unfairness authority.[173]

For an act to be unfair under the FTC Act, it is necessary (and maybe sufficient)[174] that the act "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[175] This is where the argument in *Privacy as Safety* comes into play. As argued there, threats to privacy are often threats to safety, and thus *a fortiori* a species of consumer injury.[176] It follows that commercial practices threatening privacy would qualify as unfair

168. Pub. L. 96-252, 94 Stat. 374, 378 (1980) (codified at 15 U.S.C. § 57a) ("The Commission shall not have any authority to promulgate any rule in the children's advertising proceeding pending on the date of the enactment of the Federal Trade Commission Improvements Act of 1980, or in any substantially similar proceeding on the basis of a determination by the Commission that such advertising constitutes an unfair act or practice in or affecting commerce.").

169. *See* Unfairness Policy Statement, *supra* note 127, at 1076.

170. *Id.* at 1070–76.

171. *Id.* at 1072–74.

172. Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, § 9, 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 57a). Although considerations of morality are explicitly excluded, the FTC is still permitted to "consider established public policies as evidence" demonstrating unfairness, but "[s]uch public policy considerations may not serve as a primary basis" for an unfairness determination. *Id.*

173. *Id.* at 1691–92. *See also* Magnuson-Moss Warranty Act (Federal Trade Commission Improvement Act) § 202(a), *supra* note 150, at 2193–94 (Magnuson-Moss procedures).

174. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243–249 (3rd Cir. 2015). There, addressing an argument that the codified elements of an unfairness claim "are necessary but insufficient conditions of an unfair practice," the court acknowledged that the statute "may not identify all of the requirements for an unfairness claim" but stated that the defendant failed to show "that the plain meaning of the word 'unfair' imposes independent requirements." *Id.* at 244.

175. 15 U.S.C. § 45(n).

176. *See* Froomkin & Colangelo, *supra* note 1, Part III.

practices subject to FTC authority so long as the harms are substantial and not outweighed by some countervailing benefit to consumers or competition.[177]

Many commercial practices threatening privacy constitute unfair practices for three reasons. First, commercial actions placing consumer privacy at risk "cause[] or [are] likely to cause substantial injuries to consumers" by placing their safety, health, or financial well-being at risk.[178] The term "substantial injury" requires definition. The FTC explained its understanding of substantial injury in the 1980 Policy Statement:

> First of all, the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm . . . . Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair.[179]

This explanation, which courts continue to rely upon to interpret the codified definition of an unfair practice,[180] explicitly includes risks to safety and health as potentially constituting substantial injuries.[181]

Notably, even relatively minor harms (or the risks of relatively minor harms) can qualify as substantial injuries if they are imposed on a large number of people.[182] To impose a substantial injury, an act need not result in actual harm; the imposition of an unreasonable risk of substantial harm can be sufficient.[183] Failure to adequately protect consumer privacy often poses a risk of both economic and even physical harm.[184] A widespread risk, to say nothing of actual harm, to a large group imposes the requisite substantial injury on consumers as a whole.

---

177. *See Wyndham Worldwide Corp.*, 799 F.3d at 243–249; FTC v. Neovi Inc., 604 F.3d 1150, 1155–58 (9th Cir. 2010); FTC v. D-Link Systems, Inc., 2017 WL 4150873 *3–*4 (N.D. Cal. Sept. 19, 2017); FTC v. Accusearch, Inc., 2007 WL 4356786 at *6–*8 (D. Wy. Jan. 7, 2009).

178. *See* Froomkin & Colangelo, *supra* note 1, at 163 ("Privacy enhances safety in several broad and overlapping ways: (1) it makes one physically safer; (2) it provides psychological security; (3) it makes one economically safer (and protects from some forms of invidious discrimination); and (4) it makes the exercise of various political rights safer.").

179. FTC Unfairness Policy Statement, *supra* note 127, at 1073.

180. *See*, *e.g.*, *Wyndham Worldwide Corp.*, 799 F.3d at 246 (citing FTC Unfairness Policy Statement, *supra* note 127)) (using the FTC Unfairness Policy Statement as background explaining the limits of the FTC's authority); LabMD, Inc. v. F.T.C., 894 F.3d 1221, 1229 (2018) (citing FTC Unfairness Policy Statement, *supra* note 127) (same).

181. FTC Unfairness Policy Statement, *supra* note 127, at 1073.

182. Apple Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 79 Fed. Reg. 3801, 3804 (Jan. 23, 2014) [hereinafter FTC Apple Analysis] ("It is well established that substantial injury may be demonstrated by a showing of either small harm to a large number of people or large harm in the aggregate.").

183. *Wyndham Worldwide Corp.*, 799 F.3d at 246 (citing *Int'l Harvester,* 104 F.T.C. at 1061) (finding that "unfairness claims . . . 'may also be brought on the basis of likely rather than actual injury'" and that "the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs").

184. Froomkin & Colangelo, *supra* note 1, at 163.

Second, consumers are in no position to effectively avoid privacy risks themselves, particularly in light of the increased deployment of sensors and of devices that report back to the manufacturer.[185] The growing popularity of cameras and other modes of surveillance in the public sphere leaves consumers grossly outmatched in setting boundaries on their surveillance.[186] The proliferation of the IoT provides a still greater risk to consumer privacy by creating "a complex system of surveillance" located in people's homes,[187] a risk that increases through so-called Smart Cities.[188]

"Consumers cannot avoid or protect themselves from a practice of which they are not made aware,"[189] and many consumers are unaware that the IoT system of surveillance is increasingly able to consolidate data collected from various devices through cross-tracking.[190] Using information about the consumer's "driving, home heating and cooling, food stored in a refrigerator, pulse and blood pressure,

---

185. *Cf.* FTC Apple Analysis, *supra* note 182, at 3804 ("Consumers cannot avoid or protect themselves from a practice of which they are not made aware, and companies like Apple cannot impose on consumers the responsibility for ferreting out material aspects of payment systems, as FTC enforcement actions in a variety of contexts make clear.").

186. Froomkin & Colangelo, *supra* note 1, at 144 ("With the coming of smart cities and other types of mass surveillance in the physical and electronic realms . . . , personal privacy is threatened as never before.").

187. Dalmacio V. Posadas, Jr., *After the Gold Rush: the Boom of the Internet of Things, and the Busts of Data-Security and Privacy*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 79 (2017). *See also* Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455 (2019); Jane E. Kirtley & Scott Memmel, *Rewriting the "Book of the Machine": Regulatory Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455 (2018); Sara Shahmiri, *Wearing Your Data on Your Sleeve: Wearables, the FTC, and the Privacy Implications of this New Technology*, 18 TEX. REV. ENT. & SPORTS L. 25 (2016); Nikole Davenport, *Smart Washers May Clean Your Clothes, but Hacks Can Clean Out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 279–84 (2016).

188. Predicting that "In the future, the majority of us will be living in cities, and perhaps many of us, in 'smart' or at least, not dumb, cities," Lilian Edwards describes Smart Cities as those containing

> networks of *sensors* attached to *real world objects* such as roads, cars, fridges, electricity meters, domestic appliances and human medical implants which connect these objects to digital networks . . . networks of digital communications enabling *real time data streams* which can be combined with each other and other and then be mined and repurposed for useful results; [and] *high capacity, often cloud based, infrastructure* which can support and provide storage for this interconnection of data, applications, things and people.

Lilian Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, 2 EUR. DATA PROT. L. REV. 28, 35, 31 (2016) (emphasis in original).

189. FTC Apple Analysis, *supra* note 182, at 3804.

190. FTC, CROSS-DEVICE TRACKING: AN FTC STAFF REPORT 6 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf [https://perma.cc/LE3V-53UJ] ("Because the practice of cross-device tracking is often not obvious, consumers may be surprised to find that their browsing behavior on one device will inform the ads they see on another device.").

sleep patterns, and much more"[191] gathered from different IoT devices, cross-tracking involves "platforms, publishers, and ad tech companies try[ing] to connect a consumer's activity across her smartphones, tablets, desktop computers, and other connected devices."[192] Cross-trackers are, thus, able to "collect and aggregate vast amounts of data about sites visited and apps used" by consumers without the consumers' awareness or consent.[193]

Mere awareness of IoT cross-tracking does not permit consumers to protect their information because both the process of cross-tracking and "the myriad entities that have access to, compile, and share data in the tracking ecosystem" are "opaque to consumers."[194] Even consumers who take a diligent approach to protecting their privacy will find it difficult to sufficiently educate themselves about IoT threats to privacy.[195] Privacy policies, currently "the most important source of information for consumers who are attempting to learn how companies will use their data,"[196] are woefully inadequate when it comes to informing consumers about potential privacy risks. They are difficult to find, involve "vague and unclear language," and contain "glaring omissions" related to key privacy risks.[197] In the specific context of cross-tracking, an "FTC staff[] review of privacy policies for one hundred top websites found minimal explicit disclosure to consumers about whether and how cross-device tracking occurs. Of the one hundred privacy policies reviewed, staff found only three

---

191. Kilovaty, *supra* note 187, at 472.

192. FTC, CROSS-DEVICE TRACKING: AN FTC STAFF REPORT, *supra* note 190, at § I.

193. *Id.* at 9. There are two different methods of cross-tracking: probabilistic and deterministic. The probabilistic method puts together consumer profiles based on inferences regarding "which consumer is using a device"; for example, "if a consumer's smartphone uses the same public IP address as her work computer during business hours, and then uses the same public IP address as her home computer during nonbusiness hours, an ad platform might infer that the work computer, smartphone, and home computer belong to the same consumer" despite the fact that the consumer has no reason to expect her activity on separate devices can be aggregated. *Id.* at 3.

The alternative method of cross-tracking, deterministic cross tracking, may be more apparent because it involves "a consumer-identifying characteristic, such as a login." *Id. at* 2–3. But the additional awareness of deterministic cross-tracking provides little comfort because, "[t]o improve the accuracy of their cross-device tracking models," companies that employ deterministic cross-tracking often combine it with the less-apparent probabilistic method. *Id.* Further, although many consumers are unaware that either type of cross-tracking is taking place, probabilistic cross-tracking is particularly troublesome because "consumers do not have to be logged in to any service for companies to track them probabilistic[ally]." *Id.* at i.

194. *Id.* at 8. *See also* Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, HUM. RTS. 14, 16 (2016) ("There is often also little transparency regarding, or limits on, how the data collected about users will be used.").

195. *See* FTC, CROSS-DEVICE TRACKING: AN FTC STAFF REPORT, *supra* note 190, at 8.

196. Kathryn McMahon, Note, *Tell the Smart House to Mind Its Own Business!: Maintaining Privacy and Security in the Era of Smart Devices*, 86 FORDHAM L. REV. 2511, 2528 (2018).

197. *Id.* at 2529.

policies that explicitly mentioned enabling third-party cross-device tracking on their site."[198]

The privacy problems from IoT devices working as designed can be compounded by device failures. IoT devices pose an additional risk to their users' physical privacy if their security is inadequate. If hackers gain access to the device or its controller, the hackers gain access to the consumer's physical location. Vulnerable IoT devices pose a serious risk to personal privacy because "IoT devices are not typically manufactured with robust or even minimal security standards,"[199] making them easy to hack. Hacked IoT devices become tools enabling hackers to inflict severe physical and emotional harm by, for example, draining pacemaker batteries, spying on children through baby monitors, or taking control of SUVs.[200]

Third, many of the practices putting consumer privacy at risk do not provide countervailing benefits outweighing the consumers' interest in the ability to protect their privacy. "The [FTC] has long recognized that in utilizing its authority to deem an act or practice as 'unfair' it must undertake a . . . rigorous analysis"; "[i]t is also well established that one of the primary benefits of performing a cost-benefit analysis is to ensure that government action does more good than harm."[201] When conducting the cost-benefit analysis, "the only harms and benefits on the scale are those resulting from the specific practice being challenged."[202]

The FTC provided an in-depth discussion of balancing—albeit in the context of financial harm—in an analysis of a proposed consent order with Apple, Inc.[203] "In connection with billing for children's in-app charges, Apple sometimes request[ed] a parent's iTunes password" and then stored the password for fifteen minutes, allowing further in-app purchases without additional parental consent.[204] The FTC alleged this billing practice was unfair because "Apple in many instances ha[d] not informed account holders that password entry [would] approve a charge or initiate a fifteen-minute window . . . ."[205] The proposed solution was "requir[ing] Apple to obtain express, informed consent to in-app charges before billing for such charges, and to allow consumers to revoke consent to prospective in-app charges at any time."[206]

The FTC stated (with one dissenting commissioner) that it favored the consent order because Apple's billing practice met the FTC's understanding of an

198. CROSS-DEVICE TRACKING: AN FTC STAFF REPORT, *supra* note 190, at 8.

199. Kilovaty, *supra* note 187, at 472.

200. Terry Dunlap, *The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History*, IOT FOR ALL (June 20, 2020), *https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities* [https://perma.cc/RM48-6QN2].

201. FTC Apple Analysis, *supra* note 182, at 3807–08.

202. Maureen K. Ohlhausen, *Weigh the Label, Not the Tractor: What Goes on the Scale in an FTC Unfairness Cost-Benefit Analysis?*, 83 GEO. WASH. L. REV. 1999, 2018 (2015) (arguing that the FTC's prior enforcement actions demonstrate the proper manner of conducting the unfairness balancing exercise).

203. *See* FTC Apple Analysis, *supra* note 182.

204. *Id.* at 3802.

205. *Id.*

206. *Id.* In addition, Apple had to "refund no less than $32.5 million for these in-app charges in the year following entry of the order." *Id.* at 3803.

unfair practice.[207] Noting that "Apple . . . could have prevented these unwanted purchases by including a few words on an existing prompt, without disrupting the in-app user experience," the Commission appropriately isolated the particular factors it was balancing: "What is at issue is Apple's failure to disclose the 15-minute window to parents and other account holders in connection with children's apps, not Apple's use of a 15-minute window as part of the in-app purchasing sequence."[208] Because under the order Apple had "full discretion to determine how to provide this disclosure," the burden to users or Apple would be "*de minimis*."[209]

The Apple case was about financial harm due to lack of disclosure, a trick verging on fraud. But the FTC can and should apply the same kind of analysis that justified the finding in the Apple case to a case about consumer privacy. It is true that the agency would need to demonstrate that the harm resulting from a particular act or practice is not outweighed by any countervailing benefits to consumers or competition resulting from that act or practice, and this will not always be true. But often there will be low-cost solutions available by which the FTC could address the harm associated with a particular act or practice without materially disrupting any benefits to consumers or competition. To start, the FTC could require disclosure of antiprivacy practices that, like the disclosure requirements in the Apple consent order, could provide significant privacy benefits[210] with minimal cost.

The following examples of potential FTC action illustrate how relatively simple requirements could help protect consumers against unnecessary safety risks. While there are many areas that the FTC could plausibly address in new rulemakings, two areas stand out as easy, high-value possibilities: defining standards for certain common terms and addressing the jungle of IoT privacy and security practices.

The FTC should use its experience with firms that undermine consumers' privacy interests to develop standards that would apply more generally in the marketplace.[211] The FTC's enforcement actions give it experience regarding dangers to privacy, including data breaches and misuse of the IoT.[212] However, a significant part of the FTC's privacy work consists of enforcing self-imposed corporate policies, because saying one thing while doing another is clearly deceptive

---

207. *Id.* at 3803–05.

208. *Id.* at 3803, 3805. As former FTC Commissioner Ohlhausen stated: "[W]e first examine whether the harm caused by the practice of not clearly disclosing the fifteen minute purchase window is substantial and then compare that harm to any benefits from that particular practice, namely the benefits to consumers and competition of not having a clear and conspicuous disclosure . . . ." *Id.* at 3806.

209. *Id.* at 3805 ("We firmly believe that technological innovation and fundamental consumer protections can coexist and, in fact, are mutually beneficial.").

210. There is, however, a significant body of work arguing disclosure may not be an effective solution to privacy challenges. *See, e.g.*, Froomkin, *supra* note 147, at 1733 n. 97 (collecting sources).

211. Solove & Hartzog, *supra* note 99, at 669.

212. *See generally* Elizabeth Canter & Ted Karch, *A Retrospective: the FTC's Privacy and Data Security Enforcement During the Obama Administration*, 31 ANTITRUST 34 (2017); Hartzog, *supra* note 149, at 822–23.

and probably unfair as well.[213] The FTC fines some firms caught not adhering to their policies and enters into consent orders with others in which corporations promise to avoid certain practices or take remedial action in the future,[214] although sometimes the firms avoid admitting fault.[215] Instead of its habitual piecemeal and often negotiated approach, the FTC could take this experience and use it to formulate a general rule requiring all companies in a given industry to avoid those same practices on the grounds that those practices unfairly threaten or damage consumer privacy.

The FTC also researches privacy issues related to new technology.[216] Some of the FTC's nonenforcement "tools include conducting studies and issuing reports, hosting public workshops, developing educational materials for consumers and businesses, testifying before the U.S. Congress and commenting on legislative and regulatory proposals that affect consumer privacy, and working with international partners on global privacy and accountability issues."[217] The FTC's research experience studying privacy issues and technology also puts it in a good position to craft regulations protecting personal privacy against new technological risks.

The FTC could also release a standard defining how companies must contract with data-service providers to avoid acting unfairly. Through enforcement actions, the FTC has previously indicated that companies must "(1) exercise due diligence before hiring data service providers; (2) have appropriate protections of data in their contracts with data service providers; and (3) take steps to verify that the data service providers are adequately protecting data."[218] While enforcement actions undoubtedly impact how companies contract with data-service providers, a standard clearly setting out requirements would have a greater effect.

The FTC could also take several steps toward making IoT devices safer by imposing requirements on manufacturers. Promisingly, the FTC has "embrace[d] design-based solutions, defined broadly as attempts to create or modify a technology, architecture, or organizational structure or procedure ex ante as an attempt to reduce the likelihood of a harm."[219] To bolster IoT security, the FTC could enact a rule, making mandatory what is now only its suggestion, that IoT manufacturers "[i]mplement strong encryption techniques that are available for the type of data [their] device[s] transmit[] and store[]" and "multifactor authentication

---

213. Hoofnagle, Hartzog, & Solove, *supra* note 151 (discussing how the FTC "has become a significant enforcement agency that industry pays attention to"); Solove & Hartzog, *supra* note 99, at 598–99.

214. FTC Press Release, *supra* note 103.

215. *See The Enforcers*, FTC, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/enforcers [https://perma.cc/X5SV-MPYH] (last visited Oct. 16, 2022) ("A company that signs a consent order need not admit that it violated the law . . . .").

216. FTC 2019 UPDATE, *supra* note 100, at 14–15 (listing the most recent of the seventy-five workshops the FTC has hosted since 1996).

217. *Id.* at 2.

218. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2285–86 (2015).

219. Hartzog, *supra* note 149, at 818.

to secure [their] own systems."[220] To push companies into providing more secure IoT products, the FTC could make a rule mandating that IoT manufacturers implement comprehensive privacy programs "requir[ing], among other things, the designation of an employee in charge of the program, risk assessments, design and implementation of privacy controls, diligence in working with third party contractors, and regular re-evaluation and adjustment of the program."[221]

In addition to requiring better security, the FTC could require IoT manufacturers to display clear warnings that IoT devices may be listening to or watching consumers at unexpected times. The tangible nature of IoT devices makes such warnings more effective than standard privacy policies, which are often unclear and hard to find. If IoT devices had the same type of disclosure labels the FTC currently requires on commodities[222] under the Fair Packaging and Labeling Act,[223] consumers would be better informed about risks to their privacy, allowing them to make informed decisions about privacy protection. Although the Fair Packaging and Labeling Act would not encompass IoT privacy warnings,[224] the FTC's unfairness authority could be interpreted to include the authority to require informative privacy labels to remedy consumer unawareness of privacy threats. Because people often ignore warning labels, a more effective rule would require some tangible warning signal—a light or a noise—when the device is surveilling the consumer. However, as it would require modification to the devices' design, a tangible warning requirement would likely impose higher costs on manufacturers than a mere label, so there might need to be more case-specific balancing of costs and benefits. These

---

220. FTC, CAREFUL CONNECTIONS: KEEPING THE INTERNET OF THINGS SECURE 2 (2020), https://www.ftc.gov/system/files/documents/plain-language/913a_careful_connections.pdf [https://perma.cc/B366-25RG].

221. *See* Hartzog, *supra* note 149, at 823 (citing Snapchat, Inc., 2015-1 Trade Cas. (CCH) ¶ 17115 (Dec. 23, 2014), also available at https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf [https://perma.cc/Y6J8-37DX]) (discussing the FTC's ability to require comprehensive privacy programs through consent orders).

222. 15 U.S.C. § 1459 ("The term 'consumer commodity.' Except as otherwise specifically provided in this subsection, consumer commodity means any food, drug, device, or cosmetic . . . , and any other article, product, or commodity of any kind or class which is customarily produced or distributed for sale through retail sales agencies or instrumentalities for consumption by individuals, or use by individuals for purposes of personal care or in the performance of services ordinarily rendered within the household, and which usually is consumed or expended in the course of such consumption or use.").

223. FTC, FAIR PACKAGING AND LABELING ACT: EXEMPTIONS FROM REQUIREMENTS AND PROHIBITIONS UNDER PART 500, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-packaging-labeling-act-exemptions [https://perma.cc/25YW-VATY] (last visited Oct. 16, 2022) ("The Fair Packaging and Labeling Act . . . , directs the [FTC] and the [FDA] to issue regulations requiring that all 'consumer commodities' be labeled to disclose net contents, identity of commodity, and name and place of business of the product's manufacturer, packer, or distributor.").

224. The Fair Packaging and Labeling Act does "authorize[] additional regulations where necessary to prevent consumer deception" but only when the deception relates to "descriptions of ingredients, slack fill of packages, use of 'cents-off' or lower price labeling, or characterization of package sizes." *Id.*

cost-benefit analyses likely would turn on the magnitude of the expense and the sensitivity of the data being collected.

The FTC could also require that IoT device manufacturers include an easy means of turning off monitoring functions. The FTC currently suggests that manufacturers "[b]uild security into IoT product design from the beginning, rather than as an afterthought[.]"[225] The FTC could give teeth to its suggestion that IoT manufacturers consider "what features [they] can include to ensure security"[226] by requiring basic privacy features, like an easily accessible sensor-off switch.

c. There Is No Need to Wait for Congress to Act

At times, including as recently as the Trump Administration, the FTC has suggested that it would prefer Congress give it additional powers before it undertakes any privacy-related rulemaking.[227] That position has changed: as this Article goes to press, the FTC, headed by a new Biden-appointed Chair, is signaling that it is ready for a new approach.

In December 2021, the FTC published a regulatory agenda contemplating a rulemaking designed to "curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination."[228] Then, in August 2022, the FTC published an Advance Notice of Proposed Rulemaking (ANPRM)—a prerequisite to an actual Notice of Proposed Rulemaking—requesting "public comment on the prevalence of commercial surveillance and data security practices that harm consumers."[229] In this ANPRM, the FTC notes that "consumers have little to no actual control over what happens to their information once companies collect it," and it highlights the relation between privacy and safety by observing that "[c]ompanies' collection and use of data have significant consequences for consumers' wallets, safety, and mental health."[230] The FTC will be hosting a virtual public forum to address the ANPRM in September, and comments are due in October.[231] Following that, the FTC may start an actual rulemaking under its revised Magnuson-Moss procedures.

---

225. CAREFUL CONNECTIONS: KEEPING THE INTERNET OF THINGS SECURE, *supra* note 220, at 2.

226. *Id.*

227. *See* FTC, PRIVACY AND DATA SECURITY UPDATE: 2019 1–2 (2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf [https://perma.cc/DR7V-ZZL8] ("To better equip the Commission to meet its statutory mission to protect consumers, the FTC has also called on Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC. The requested legislation would expand the agency's civil penalty authority [and] provide the agency with targeted rulemaking authority . . . .").

228. FTC, STATEMENT OF REGULATORY PRIORITIES 2 (2021), https://www.reginfo.gov/public/jsp/eAgenda/StaticContent/202110/Statement_3084_FTC.pdf [https://perma.cc/CUH8-CGQR].

229. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022).

230. *Id.* at 51,274–75.

231. *Id.* at 51,285–86.

Meanwhile, Congress is considering potential bipartisan privacy legislation, the American Data Privacy and Protection Act (ADPPA).[232] Opinions differ on the value of the proposal. The former Clinton Administration Privacy Czar Peter Swire called it a "big deal."[233] But privacy groups swooped in to note its flaws, notably the extensive preemption of stronger state laws.[234] Reports suggested that many Republicans in the House, and perhaps also a few powerful Democrats in the Senate, thought the draft went too far.[235] As Peter Swire noted, "It's always a good bet that broad privacy legislation will fail to pass."[236] Indeed, ADPPA did not pass before the 2022 election recess, so hopes of passage in this session of Congress now turn on whether ADPAA can find a place in what promises to be a very crowded lame-duck legislative calendar.[237]

Fortunately, as described above, much can be done without waiting for additional privacy legislation from Congress. As Chris Hoofnagle has noted, "the FTC could go further in policing privacy practices based on precedent in advertising and other cases."[238] Indeed, the FTC already has broad regulatory authority, and as noted above, many privacy-destructive practices are easily characterized as unfair or deceptive. The FTC's extensive experience with privacy issues should enable it to issue effective rules aimed at protecting personal privacy against those unfair and deceptive practices. Rather than wait for additional direction from Congress, the

---

232. *See generally* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2d Sess. 2022), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf [https://perma.cc/U22C-3KMW].

233. Peter Swire, *The Bipartisan, Bicameral Privacy Proposal Is a Big Deal*, LAWFARE BLOG (June 9, 2022, 2:12 PM), https://www.lawfareblog.com/bipartisan-bicameral-privacy-proposal-big-deal [https://perma.cc/37J9-8G45].

234. *E.g.*, Letter to Hon. Frank Pallone Jr. et al., *Re: Hearing on Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security*, ELECTRONIC FRONTIER FOUNDATION (June 13, 2022), https://www.eff.org/files/2022/06/14/2022.06.13_eff_letter_to_house_enc_re._hearing_on_protecting_americas_consumers_.pdf [https://perma.cc/W4XD-K8ZX].

235. Dell Cameron, *Oof, the Prospects of That Big New Privacy Bill in Congress Look Grim*, GIZMODO (June 24, 2022), https://gizmodo.com/american-data-privacy-protection-act-faces-congress-c-1849102270 [https://perma.cc/42QA-NHJ3] (reporting that Senate Majority Leader Chuck Schumer opposes the bill).

236. Swire, *supra* note 233. *See also* Cameron, *supra* note 235 (bill "looks now like it's being blindfolded and handed a last cigarette").

237. *See* Andrew Solender, *Congress Barrels Toward "Extremely Busy" Lame-Duck Session,* AXIOS (Sept. 29, 2022), https://www.axios.com/2022/09/30/lame-duck-session-congress-priorities [https://perma.cc/UN4Z-7JAV]; *The American Data Privacy and Protection Act*, AM. BAR ASS'N (Aug. 30, 2022), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/ (last visited Oct. 18, 2022) [https://perma.cc/4ZMT-WVNC] (opining that the legislation is unlikely to pass before the conclusion of the 117th Congress on January 3, 2023, but noting that it "could become a priority issue once the new Congress convenes, regardless of the results of the forthcoming midterm elections").

238. HOOFNAGLE, *supra* note 94, at 119.

FTC could use its existing authority and experience to make rules protecting the privacy of vulnerable consumers.[239]

C. The Consumer Product Safety Commission (CPSC)

The CPSC could do more to protect consumers from the privacy threats posed by modern consumer devices, specifically those devices that make up the IoT. Congress charged the CPSC with protecting consumers from unreasonable threats of injury from consumer products.[240] In the past three years, the CPSC has correctly recognized that many products, particularly those that are part of the IoT, pose a risk of injury to consumers.[241] Unfortunately, in addressing the risks associated with IoT devices, the CPSC has narrowed its focus to risks of strictly physical injury.[242] To keep consumers safe, the CPSC could adopt a broader understanding of its safety mission and use its authority to issue standards aimed at preventing unreasonable threats to consumer privacy from IoT devices.

1. The CPSC Has Authority to Make Rules Protecting Consumer Privacy

Congress created the CPSC in 1972 to protect the public "against unreasonable risks of injury associated with consumer products."[243] Specifically, Congress believed the "complexities of consumer products and the diverse nature and abilities of consumers using them frequently result in an inability of users to anticipate risks and to safeguard themselves adequately."[244] The Consumer Products Safety Act (CPSA) was meant "(1) to protect the public against *unreasonable risks of injury* associated with consumer products; (2) to assist consumers in evaluating the comparative safety of consumer products; (3) to develop uniform safety standards for consumer products . . . ; and (4) prevention of product related deaths, illnesses, and injuries."[245]

---

239. *See* Davis, *supra* note 99, at 812 ("Although the political parties share a common goal, they have failed to translate their conflicting data security priorities into law, suggesting that the FTC holds an institutional advantage over the legislative branch.").

240. Consumer Product Safety Act, Pub. L. No. 92-573, 86 Stat. 1207 (1972) (codified as amended in scattered sections of 15 U.S.C.).

241. *See generally* The Internet of Things and Consumer Products Hazards, 83 Fed. Reg. 13,122 (March 27, 2018); CONSUMER PROD. SAFETY COMM'N, STATUS REPORT ON THE INTERNET OF THINGS (IoT) AND CONSUMER PRODUCT SAFETY (Sept. 25, 2019) [hereinafter CPSC STATUS REPORT]; ELLIOT F. KAYE & JONATHAN D. MIDGETT, A FRAMEWORK OF SAFETY FOR THE INTERNET OF THINGS: CONSIDERATIONS FOR CONSUMER PRODUCT SAFETY (Jan. 31, 2019) https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019.pdf.

242. *See* The Internet of Things and Consumer Products Hazards, *supra* note 241 ("We do not consider personal data security and privacy issues that may be related to IoT devices to be consumer product hazards that CPSC would address."); CPSC STATUS REPORT, *supra* note 241, at 2 ("CPSC does not consider personal data protection and privacy to be consumer product hazards that we would address, absent an associated unreasonable risk of injury."); KAYE & MIDGETT, *supra* note 241, at 1 ("This framework is not specifically intended to address issues related to the personal privacy . . . .").

243. Consumer Product Safety Act, Pub. L. No. 92-573, 86 Stat. 1207 (1972) (codified at 15 U.S.C. § 2051(a)(3)).

244. *Id.* at § 2051(a)(2)).

245. *Id.* at § 2051(b) (emphasis added).

Since Congress enacted the CPSA, the complexity of consumer products has grown exponentially, and so has the need for consumer protection against their risks. Consumers' inability to understand the risks associated with consumer products is particularly acute in connection with the IoT.[246] As more devices are connected to the Internet, consumers more frequently come into contact with devices that inconspicuously compromise their privacy in ways most consumers cannot detect and do not understand.[247] Because consumer IoT devices pose the types of risk contemplated in the CPSA, the CPSC could use its authority under that Act to help protect people's privacy against the rapidly developing IoT rather than hewing solely to its focus on things that can cause physical injury.

One of the CPSC's tools under the CPSA is the authority to "promulgate consumer products safety standards" when "reasonably necessary to prevent or reduce an unreasonable risk of injury associated with [a consumer] product."[248] To issue consumer product safety standards, the CPSC must find, among other things, "that the rule . . . is reasonably necessary to eliminate or reduce an unreasonable risk of injury," [249] defined as "risk of death, *personal injury*, or serious or frequent illness." [250] Additionally, the standards must consist of "[r]equirements expressed in terms of performance requirements" or "[r]equirements that a consumer product be marked with or accompanied by clear and adequate warnings or instructions, or requirements respecting the form of warnings or instructions."[251]

Although the CPSC has yet to acknowledge it, privacy risks posed by consumer IoT products[252] fall tidily under the CPSC's authority to regulate the risk of personal injury because privacy infringements can threaten the physical well-being of consumers.[253] Many consumer IoT products pose unreasonable risks to consumer safety by compromising physical privacy.[254]

The IoT can also threaten consumer well-being by putting consumer information at risk due to poor security. As the CPSC has acknowledged, "[i]n the current world of IoT-connected consumer products, the concept of 'unreasonable

---

246. *See* Kathryn McMahon, *supra* note 196, at 2528. *See also* Williams, *supra* note 194, at 16 ("There is also often little transparency regarding, or limits on, how the data collected about users will be used.").

247. Froomkin & Colangelo, *supra* note 1, at 163.

248. 15 U.S.C. § 2056(a). Developing such standards is an important tool for the CPSC; "[s]ince its inception, the CPSC has issued numerous safety standards for products as varied as bicycles, children's toys, matchbooks, swimming pools, garage door openers, portable generators, and all-terrain vehicles." Edward M. Crane et al., *U.S. Consumer Protection Law: A Federalist Patchwork*, 78 DEF. COUNS. J. 305, 313 (2011).

249. 15 U.S.C. § 2058(f)(3).

250. *Id.* § 2052(a)(14) (emphasis added).

251. *Id.* § 2056(a).

252. "[The CPSC's] focus is on the Consumer IoT and the consumer products that are connected to the Internet or other network directly or indirectly, or *connected products*." CPSC STATUS REPORT, *supra* note 241, at 6.

253. *See generally* Froomkin & Colangelo, *supra* note 1, at 163.

254. *See generally* Woodrow Hartzog & Evan Selinge, *The Internet of Heirlooms and Disposable Things*, 17 N.C.J.L. & TECH. 581 (2016); WOODROW HARTZOG, PRIVACY'S BLUEPRINT THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).

risk' shares a nexus with data security."[255] Security weaknesses[256] in the IoT can lead a consumer product to become "hazardized"[257] on account of "[m]alicious hacking."[258] As the CPSC itself explained, "[e]xamples include: the robotic vacuum that loses its way and falls down the stairs onto a small child due to a poorly designed third-party app or the connected heating system in the home of an elderly resident that shuts down on a bitterly cold winter day after the software is hacked."[259] Concerns about IoT data security encompass "all of the data stored in, or moving in or out of a connected device that could impact the safety of the product."[260] The CPSC has identified "[o]perational instructions (software)," as well as "[c]onsumer originated data (*e.g.*, biometrics, settings and preferences, multiple-user identification)," and "[e]nvironmental metrics (*e.g.*, location, temperature, atmosphere, energy)" as categories of consumer information that may be vulnerable to flaws in IoT security.[261]

The IoT also poses an unreasonable risk of injuries associated with privacy infringement because consumers generally lack the ability to properly protect their own privacy. There is little that most consumers are able to do to prevent a hacker from inflicting physical harm through consumer IoT devices[262] because "a consumer could not anticipate the data security defect that allowed the change in the product and the resulting hazardous condition."[263] More generally, the complexity of privacy risks associated with the IoT leaves most users unable "to anticipate risks and to safeguard themselves adequately."[264] Protecting against these risks is, or should be, at the heart of the CPSC's mission to protect consumers "against unreasonable risks

---

255. CPSC STATUS REPORT, *supra* note 241, at 7.

256. *See generally* Dunlap, *supra* note 200.

257. The CPSC defines "[h]azardization [as] the process by which a product, which would otherwise be safe, poses a danger to consumers when connected to the Internet is subjected to unauthorized, imprudent, or anomalous data transfer interference or manipulation of operational code or consumer-originated data, with the potential to cause injury or death." CPSC STATUS REPORT, *supra* note 241, at 5 n.3.

258. *Id*. at 8.

259. *Id.* In addition, the FTC included the following example in its comments submitted to the CSPC regarding the IoT:

> [A] car's braking systems might fail when infected with malware, carbon monoxide detectors or fire alarms might stop working with the loss of connectivity, and corrupted or inaccurate data on a medical device might pose health risks to a user of the device. Consumers' physical safety could also be at risk if an intruder had access to a connected lock, garage door, or burglar alarm.

FTC, COMMENTS OF THE STAFF OF THE FEDERAL TRADE COMMISSION'S BUREAU OF CONSUMER PROTECTION (June 15, 2018), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf [https://perma.cc/J8UL-FPAM].

260. CPSC STATUS REPORT, *supra* note 241, at 9.

261. *Id.*

262. For some examples of such harms, *see* Dunlap, *supra* note 200.

263. CPSC STATUS REPORT, *supra* note 241, at 8.

264. Consumer Product Safety Act, Pub. L. No. 92-573, 86 Stat. 1207 (1972) (codified at 15 U.S.C. § 2051(a)(2)).

of injury associated with consumer products[.]"[265] That some of the risks relate to intangible information harms is of no relevance because the law recognizes that "personal injury" is a broad concept that encompasses both physical and nonphysical harm.[266]

As of this writing, early in the Biden administration, the CPSC has largely deferred to other agencies about most cybersecurity and privacy issues.[267] At the same time, however, the CPSC has engaged in serious research related to the IoT, although the focus remains on the direct risk of physical injury.[268] This work includes gathering feedback on a potential framework to address the IoT, albeit "not specifically intended to address issues related to the personal *privacy* or data *confidentiality* of information,"[269] and actively evaluating the agency's possible role in keeping consumers safe from potential IoT harm.[270] The CPSC should not delay in expanding its efforts to keep consumers safe from unreasonable risks to their privacy. Some of the following regulatory actions would be an effective starting point.

2. Examples of CPSC Rules that Would Protect Privacy

To make IoT privacy safety a priority, the CPSC could devote more resources to developing relevant safety standards. Specifically, it could, as Andrea Matwyshyn suggests, "organize a working group around issues of IoT hardware and software safety, culminating in rulemaking that focuses on IoT consumer products."[271] At a minimum, these new safety standards could require that manufacturers implement basic security measures aimed at keeping the consumer safe from physical and privacy harm and also keep the consumer's information safe from unauthorized access, whether by design or by hacking poorly secured IoT devices.

After promulgating basic privacy-related safety standards, the CPSC could require that IoT manufacturers obtain privacy certification through a process

---

265. *Id.*

266. *See* Froomkin & Colangelo, *supra* note 1, Section III (providing examples of how "in many cases U.S. law already recognizes and protects privacy in order to protect the safety of individuals in a wide variety of circumstances," including circumstances involving the threat of nonphysical harm).

267. *See* CPSC STATUS REPORT, *supra* note 241, at 6 ("Data security, privacy and consumer product safety have traditionally been addressed independently by various federal agencies with jurisdiction in these areas. The CPSC has not considered data security and privacy issues related to consumer products to be hazards we would address, absent an associated unreasonable risk of injury.").

268. *See, e.g.,* Consumer Product Safety Commission, *supra* note 243, at 13,122 (focusing on traditional hazards associated with IoT devices, like "[f]ire, burn, shock, tripping or falling, laceration, contusion, and chemical exposure."); KAYE & MIDGETT, *supra* note 241; CPSC STATUS REPORT, *supra* note 241.

269. KAYE & MIDGETT, *supra* note 241, at 1.

270. CPSC STATUS REPORT, *supra* note 241, at 8.

271. Andrea M. Matwyshyn, *The Internet of Bodies*, 61 WM. & MARY L. REV. 77, 135–36 (2019). Matwyshyn also suggests the CPSC should "contribute a cross-detailed team to the FTC's new technology practices group." *Id.*

subjecting their devices to third-party testing.[272] The CPSC could accredit third-party researchers to "essentially employ hacking techniques for the purpose of enhancing security—in other words, [the researchers would] think and act like a hacker *for* the company in order to ward off future criminal hacking."[273]

Furthermore, in cooperation with the FTC, the CPSC could also require that IoT manufacturers provide more clarity surrounding their security standards.[274] In addition to "improv[ing] transparency and provid[ing] consumers with information to better evaluate the safety and security of their IoT products," public disclosures would enable the FTC to "use its authority under the FTC Act to take action against companies that misrepresent their security practices."[275]

D. The Food & Drug Administration (FDA)

The FDA regulates, among other things, the sale and use of medical devices.[276] Today, a growing number of these medical devices have internet-connectivity capabilities that make them part of an Internet of Medical Things ("IoMT").[277] The IoMT thus poses new challenges to the FDA's regulation of safety

---

272. *Cf.* Heather Bramble & Thomasina E. Poirot, *The Internet of Things, Product Safety, and Product Liability: A Risky Combination*, VENABLE (May 23, 2018), https://www.allaboutadvertisinglaw.com/2018/05/the-internet-of-things-product-safety-and-product-liability-a-risky-combination.html [https://perma.cc/L4E9-NWJE] (describing how, at the CPSC's 2018 public hearing on IoT issues, "consumer activists described the [safety] situation as 'urgent' and pressed the Commissioners to provide a certification process for IoT devices and stronger mandatory regulations for manufacturers that incorporate software technologies into their products"). The CPSC currently requires certification through third party testing for certain children's products; this involves accrediting third-party laboratories qualified to carry out testing. *Third Party Testing*, CONSUMER PROD. SAFETY COMM'N, https://www.cpsc.gov/Business--Manufacturing/Testing-Certification/Third-Party-Testing (last visited Nov. 16, 2022) [https://perma.cc/C3M9-DFK6] ("Federal law requires that every children's product be tested by a third party, CPSC-accepted laboratory for compliance with the applicable federal children's product safety requirements.").

273. Kilovaty, *supra* note 187, at 462 (arguing that "outsourcing some of the [IoT] vulnerability discovery to third-party actors—security researchers—would bolster IoT security").

274. FTC, COMMENTS OF THE STAFF OF THE FEDERAL TRADE COMMISSION'S BUREAU OF CONSUMER PROTECTION 10 (June 15, 2018) ("In addition, to the extent that the CPSC considers certification requirements for IoT devices, the CPSC should consider requiring manufacturers to publicly set forth the standards to which they adhere.").

275. *Id.* ("Examples of enforceable statements to consumers could include statements on websites, on a retail packaging, on the device itself, or in the user interface of the device.").

276. 21 U.S.C. § 351.

277. *See* Andrew Steger, *How the Internet of Medical Things is Impacting Healthcare*, HEALTHTECH (Jan. 16, 2020), https://healthtechmagazine.net/article/2020/01/how-internet-medical-things-impacting-healthcare-perfcon [https://perma.cc/L6MY-B3LE] (describing the internet of medical things ("IoMT") as "a connected infrastructure of medical devices, software applications, and health systems and services"); Greg Reh, *Eight IoT Barriers for Connected Medical Devices and How to Overcome Them,* DELOITTE (Aug. 14, 2018), https://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/health-care-current-august14-2018.html [https://perma.cc/XUM5-DUU9] ("Within the next five

in medical devices.[278] In particular, devices sold for consumers to monitor their own biological functions or medical conditions can fall outside the FDA's current regulatory ambit. Worse, when users share information collected by these devices via cell phone apps or social media, the information shared is commonly not covered by medical privacy regulation.[279] Further, vulnerable IoMT devices may provide intruders with unauthorized access to both medical data and the users themselves.[280] A 2019 survey found that "80% of organizations' IoT devices that they manufacture or use have experienced a cyberattack in the past 12 months."[281] Unauthorized access to medical data is increasingly dangerous in part due to the ongoing digitization of increasing amounts of medical information.[282] And direct, unauthorized access to the users through an IoMT device, like a pacemaker or insulin pump, could be fatal.[283] The FDA should be using its authority to regulate medical devices to protect users from privacy threats that are not only unsafe but potentially fatal.

---

years, medical technology companies anticipate that 68 percent of their devices will be connected through IoT.").

278. *Irdeto Global Connected Industries Cybersecurity Survey: IoT Cyberattacks are the Norm, the Security Mindset Isn't*, IRDETO (2019), https://resources.irdeto.com/media/global-connected-industries-cybersecurity-survey-1?page=%2Fwhite-papers-e-books-reports&widget=61a00432c044d513b464dac5 [https://perma.cc/CH4B-Y57H].

279. *See* Alexis Guadarrama, *Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry*, 55 HOUS. L. REV. 999 (2018) ("amount of protection health data receives depends on who holds the data, not the type of information being held"); Katharine A. Van Tassel & J.T. O'Reilly, *Regulation of Mobile Devices*, 2 FOOD AND DRUG ADMINISTRATION § 18:196 (4th ed. 2022) (stating "many health apps currently are subject to FDA 'enforcement discretion,' which translates to 'we would enforce if this product or its claims of benefit had caused serious health concern but not if it is used for a routinely benign purpose'").

280. IRDETO, *supra* note 278, at 5 ("Of those organizations [that have experienced a cyberattack], 90% experienced an impact as a result of the cyberattack. This could include operational downtime, compromised customer data, end-user safety, brand or reputational damage, a loss of customers or stolen intellectual property.").

281. *Id.* at 3.

282. *See* Jeff Hecht, *Fixing a Broken Record*, 573 NATURE S114 (2019), https://media.nature.com/original/magazine-assets/d41586-019-02876-y/d41586-019-02876-y.pdf [https://perma.cc/7SB6-GJHR] ("[I]n 2017, 96% of hospitals and 86% of physicians' offices in the United States had access to electronic health records."); Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon [https://perma.cc/T3YT-FG77] ("Although stolen health data can be used to carry out a variety of crimes, two scenarios are detrimental: leveraging details specific to a disease or terminal illness, and long-term identity theft.").

283. *See, e.g.*, Peter Jaret, *Exposing Vulnerabilities: How Hackers Could Target Your Medical Devices*, AAMC (Nov. 12, 2018), https://www.aamc.org/news-insights/exposing-vulnerabilities-how-hackers-could-target-your-medical-devices [https://perma.cc/A6K8-3242] (describing the relatively easy process of hacking an insulin pump to "deliver a lethal dose to a patient").

1. The FDA Has Authority to Make Rules Protecting Patients' Privacy

In the Food and Drugs Act of 1906, Congress authorized the Bureau of Chemistry of the Department of Agriculture (which became the FDA in 1930)[284] to make "examinations of specimens of foods and drugs" to determine "whether such articles are adulterated or misbranded."[285] Then, in 1938, Congress amended the Food and Drugs Act to include medical devices and cosmetics.[286] Congress defined "devices" broadly as "instruments, apparatus, and contrivances, including their components, parts, and accessories, intended (1) for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man or other animals; or (2) to affect the structure or any function of the body of man or other animals."[287] Giving the Secretary of Agriculture[288] "[t]he authority to promulgate regulations for the efficient enforcement of this Act,"[289] Congress prohibited "[t]he introduction" or "manufacture" of "any food, drug, device, or cosmetic that is adulterated or misbranded."[290]

In 1976, Congress amended the Federal Food, Drug, and Cosmetic Act "to provide for the safety and effectiveness of medical devices intended for human use."[291] It set up a risk-based classification system designed to obtain "reasonable assurance of [each device's] safety and effectiveness."[292]

---

284. In 1927, the Bureau of Chemistry's regulatory functions were moved into the Food, Drug, and Insecticide Administration; then, in 1930, the Food, Drug, and Insecticide Administration's name was shortened to the FDA. *Milestones in U.S. Food and Drug Law*, FOOD & DRUG ADMIN. (last updated Jan. 31, 2018), https://www.fda.gov/about-fda/fda-history/milestones-us-food-and-drug-law [https://perma.cc/67XH-RHTF].

285. Food and Drugs Act, June 30, 1906, c. 3915, 34 Stat. 768 (codified as amended in 21 U.S.C.).

286. Federal Food, Drug, and Cosmetic Act, Pub. L. 717, 52 Stat. 1040, June 25, 1938 (codified as amended at 21 U.S.C. § 300 et seq.).

287. *Id.* § 201(h) (codified as amended at 21 U.S.C. 321). The definition of device has been expanded to include certain types of software designed to serve a specific medical purpose. IMDRF SAMD WORKING GROUP, *Software as a Medical Device (SaMD): Key Definitions* (2013), http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf [https://perma.cc/XP2X-CC6Q] ("The term 'Software as a Medical Device' (SaMD) is defined as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device.")

288. The FDA remained part of the Department of Agriculture until 1940. *Milestones in U.S. Food and Drug Law*, FOOD & DRUG ADMIN. (last updated Jan. 31, 2018), https://www.fda.gov/about-fda/fda-history/milestones-us-food-and-drug-law [https://perma.cc/528B-85HR].

289. Federal Food, Drug, and Cosmetic Act § 701(a), Pub. L. 717, 52 Stat. 1040, June 25, 1938 (codified as amended at 21 U.S.C. § 371).

290. Federal Food, Drug, and Cosmetic Act § 301, Pub. L. 717, 52 Stat. 1040, June 25, 1938 (codified as amended at 21 U.S.C. § 331). A device was misbranded "[i]f its labeling [was] false or misleading in any particular"; a device was adulterated "(1) if it consist[ed] in whole or in part of any filthy, putrid, or decomposed substance; or (2) if it ha[d] been prepared, packed, or held under insanitary conditions . . . whereby it may have been rendered injurious to health." *Id.* §§ 501, 502.

291. The Medical Device Amendments of 1970, Pub. L. 94-295, 90 Stat. 539, May 28, 1976 (codified as amended at 21 U.S.C. § 360 et seq.).

292. *Id.*

To ensure that IoMT devices are "safe and effective," the FDA should require adequate protection for physical privacy and medical data. IoMT devices threaten data privacy by offering potential gateways to comprehensive collections of medical data.[293] Security failures exacerbate the problem: as noted above, the majority of manufacturers and users of IoMT devices have experienced cybersecurity attacks.[294] These cybersecurity attacks could enable intruders "to grab electronic health records, release software viruses that could disrupt hospital operations, and launch a ransomware attack."[295] After gaining access to medical data, intruders could use that information to harm individuals by "leveraging details specific to a disease or terminal illness, [or carrying out] long-term identity theft."[296] An intruder with sensitive medical information that a patient wants to keep private can use the information to obtain "a financial payoff extorted from the hacked individual."[297] The potential for medical identity theft, which the FTC describes as (1) using "another person's name or insurance information to get medical treatment, prescription drugs or surgery" or (2) using "another person's information to submit false bills to insurance companies,"[298] can have long-term ramifications "because health data can't be changed."[299] "A thief may use [a victim's] name or health insurance numbers to see a doctor, get prescription drugs, file claims with [the victim's] insurance provider, or get other care," leaving the victim with serious credit problems and thousands of dollars in debt.[300]

IoMT devices that permit unauthorized access to users themselves are especially dangerous. In 2011, an experimenter found that "it wasn't difficult to take control of an insulin pump and deliver a lethal dose to a patient."[301] The experimenter also demonstrated how "[u]sing a laptop, . . . it was possible to send a lethal electric shock to a patient via pacemaker."[302] Subsequently, the FDA identified a serious cybersecurity vulnerability in insulin pumps that triggered "a Class I recall, the most serious type of recall."[303] The FDA found that the lack of

---

293. Jaret, *supra* note 283.

294. IRDETO, *supra* note 278, at 3 (finding that "that "80% of organizations' IoT devices that they manufacture or use have experienced a cyberattack in the past 12 months").

295. Jaret, *supra* note 283.

296. Steger, *supra* note 282.

297. *Id.*

298. FTC, MEDICAL IDENTITY THEFT (Jan. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf [https://perma.cc/V8TW-RXKN].

299. Steger, *supra* note 282.

300. FTC, MEDICAL IDENTITY THEFT (Sept. 2018), https://www.consumer.ftc.gov/articles/0171-medical-identity-theft [https://perma.cc/383Y-C5A8]. *See also* Steger, *supra* note 277 (describing a medical identity theft victim left with "bills [that] totaled nearly $20,000").

301. Jaret, *supra* note 283.

302. *Id.*

303. *Medtronic Recalls Remote Controllers for MiniMed Insulin Pumps for Potential Cybersecurity Risks*, FOOD & DRUG ADMIN. (last updated Nov. 18, 2019), https://www.fda.gov/medical-devices/medical-device-recalls/medtronic-recalls-remote-controllers-minimed-insulin-pumps-potential-cybersecurity-risks ("Using specialized

adequate cybersecurity measures meant using the insulin pump could "cause serious injuries or death."[304]

The FDA's mandate to ensure medical devices have controls "sufficient to provide reasonable assurance of the safety and effectiveness"[305] calls for heightened focus on dangerous privacy threats related to the IoMT. The FDA has taken several steps towards addressing privacy concerns,[306] including the release of nonbinding guidance related to addressing cybersecurity risks,[307] the development of a "Software Precertification (Pre-Cert) Program"[308] to regulate medical software

---

equipment, an unauthorized person could instruct the pump to either over-deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or stop insulin delivery, leading to high blood sugar and diabetic ketoacidosis, even death.").

304. *Id.*

305. 21 U.S.C. § 360c.

306. In addition to its work with IoMT devices, the FDA has also helped safeguard privacy through promulgated electronic records regulations that "provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records." FOOD & DRUG ADMIN., GUIDANCE FOR INDUSTRY PART 11, ELECTRONIC RECORDS; ELECTRONIC SIGNATURES – SCOPE AND APPLICATION (Aug. 2003), https://www.fda.gov/media/75414/download [https://perma.cc/CM5H-SMFH]. According to draft guidance released in 2017, the regulations cover "[r]ecords required for clinical investigations of medical products" that are (1) "necessary for the FDA to reconstruct a study" or (2) "relied on to perform regulated activities." FOOD & DRUG ADMIN., USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES IN CLINICAL INVESTIGATIONS UNDER 21 CFR PART 11 – QUESTIONS AND ANSWERS (June 2017), https://www.fda.gov/media/105557/download [https://perma.cc/AQ7E-FN86]. The regulations also cover records "submitted to FDA in electronic format." *Id.* The FDA's electronic records regulations require regulated entities to "employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records"; the regulations explicitly require procedures aimed at "[l]imiting system access to authorized individuals." 21 C.F.R. § 11.10.

307. *See generally* FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS (Sept. 27, 2019), https://www.fda.gov/media/80958/download [https://perma.cc/25TL-DX3A]; FOOD & DRUG ADMIN., CYBERSECURITY IN MEDICAL DEVICES: QUALITY SYSTEM CONSIDERATIONS AND CONTENT OF PREMARKET SUBMISSIONS DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Oct. 18, 2018), https://www.fda.gov/media/119933/download [https://perma.cc/DNB3-ZVMW];FOOD & DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (Dec. 28, 2016), https://www.fda.gov/media/95862/download [https://perma.cc/2DAR-G5QK]; FOOD & DRUG ADMIN., GUIDANCE TO INDUSTRY: CYBERSECURITY FOR NETWORKED MEDICAL DEVICES CONTAINING OFF-THE-SHELF (OTS) SOFTWARE (Jan. 14, 2005), https://www.fda.gov/media/72154/download [https://perma.cc/X9LC-NL7V]. The FDA is also planning to release new cybersecurity guidance later this year. Nancy Crotti, *New FDA Medtech Cybersecurity Chief: Guidance to Debut in 2021*, MASSDEVICE (Feb. 19, 2021), https://www.massdevice.com/new-fda-medtech-cybersecurity-chief-guidance-to-debut-in-2021/ [https://perma.cc/3GCJ-4GBV].

308. FOOD & DRUG ADMIN., DEVELOPING THE SOFTWARE PRECERTIFICATION PROGRAM: SUMMARY OF LEARNINGS AND ONGOING ACTIVITIES (Sept. 2020), https://www.fda.gov/media/142107/download [https://perma.cc/9TL4-S4FD]

directly, and the establishment of a new (but temporary) position devoted to addressing cybersecurity issues.[309] Building on these efforts to bolster privacy protection, the FDA should use its regulatory authority to develop standards aimed at protecting against dangerous privacy risks.

2. Examples of FDA Rules that Would Protect Privacy

As an important first step, the FDA could expand the scope of the devices it regulates. Currently, the FDA does not exercise its regulatory authority over wearable products that "(1) are intended for only general wellness use, as defined in this guidance, and (2) present a low risk to the safety of users and other persons."[310] This exclusion puts many popular devices—which collect large amounts of health data—beyond the FDA's regulatory oversight.[311] Even if these devices cannot directly kill the user, as might the riskiest implantables, wearables still raise cybersecurity concerns,[312] and the FDA could pursue a more expansive use of its authority to protect patients' privacy.

The FDA could also enact aspects of its cybersecurity guidance as mandatory requirements. Currently, with regard to premarket approval of devices using medical software, the FDA guidance states that it "may make it more likely

---

(acknowledging that the "FDA's traditional approach for the regulation of hardware-based medical devices is not well suited for the faster and more iterative design, development, and validation techniques used to develop high quality, safe and effective software, including Software as a Medical Device (SaMD)").

309. *FDA Appoints Kevin Fu as Its First Director of Medical Device Security*, HIPAA J. (Feb. 5, 2021), https://www.hipaajournal.com/fda-appoints-kevin-fu-as-its-first-director-of-medical-device-security/ [https://perma.cc/M8QM-HTAG] (describing the one-year term of a new "Director of Medical Device Security" meant to "help to develop the CDRH cybersecurity programs, public-private partnerships, and premarket vulnerability assessments to ensure the safety of medical devices including insulin pumps, pacemakers, imaging machines, and healthcare IoT devices and protect them against digital security threats").

310. FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES (Sept. 27, 2019), https://www.fda.gov/media/90652/download [https://perma.cc/9NX6-WXCG]. Similarly, regarding SaMD, the FDA excludes "software functions that: 1. Help patients (i.e., users) self-manage their disease or conditions without providing specific treatment or treatment suggestions; or 2. Automate simple tasks for health care providers." FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS , *supra* note 307.

311. *See FDA Says It Won't Regulate FitBit, Many Other Fitness Wearables*, ADVISORYBOARD (Aug. 18, 2016), https://www.advisory.com/en/daily-briefing/2016/08/18/fda-says-it-wont-regulate-fitbit [https://perma.cc/JM7V-ZADX]. The FDA has, however, gotten involved in approving Fitbit's ECG app designed to "determine[] the presence of atrial fibrillation (Afib) or sinus rhythm on a classifiable waveform." Letter from Jessica E. Paulson, FDA, to Shruti Rajagopalan, Fitbit, Inc. (Sept. 11, 2020), https://www.accessdata.fda.gov/cdrh_docs/pdf20/K200948.pdf [https://perma.cc/3WPH-EDJU].

312. *See* Marianne Kolbasuk McGee, *Fitbit Hack: What Are the Lessons?*, DATABREACH (Jan. 11, 2016), https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793 [https://perma.cc/3ZXS-VPGK] (describing a Fitbit hack that gave the intruders "access to customer data, including GPS history, which shows where a person regularly runs or cycles, as well as data showing what time a person usually goes to sleep").

that FDA will find [that a manufacturer's] device meets its applicable statutory standard for premarket review"[313] if the manufacturer follows the FDA's "recommended design implementations of authentication, authorization, and encryption."[314] The FDA could make this suggestion into a requirement that manufacturers must meet before getting premarket approval for their IoMT devices.

The FDA could also make its recommended labeling practices mandatory. FDA draft guidance notes that "informing end-users of relevant security information may be an effective way to comply with labeling requirements,"[315] and it provides a helpful list of recommended labeling practices, including labeling medical devices with: (1) "[d]evice instructions . . . related to recommended cybersecurity controls"; (2) "[a] description of the device features that protect critical functionality"; (3) "[a] description of how forensic evidence is captured"; and (4) "instructions for users on how to respond upon detection of a cybersecurity vulnerability or incident."[316]

Further, the FDA could require that device manufacturers submit risk-management reports to obtain premarket approval. In crafting and submitting this report, manufacturers would be required to take "a comprehensive approach that considers both security and safety risk analysis in a meaningful way."[317] By requiring manufacturers to submit a thorough, comprehensive report, the FDA could encourage manufacturers to take cybersecurity concerns more seriously. An initial reporting requirement would also allow the FDA to more easily monitor a manufacturer's efforts going forward.

Indeed, all medical-device manufacturers' responsibility to create safe medical products and to report shortcomings could continue throughout the life of the device. The FDA currently recommends that manufacturers report "information concerning cybersecurity vulnerabilities, and the device changes and compensating controls implemented in response to this information . . . to FDA in a periodic (annual) report."[318] The FDA could turn this recommendation into a requirement that IoMT manufacturers regularly update the FDA on developing cybersecurity issues and efforts to combat those issues.

---

313. FDA, DRAFT GUIDANCE: CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (April 8, 2022), https://www.fda.gov/media/119933/download [https://perma.cc/Z57A-AGTB].

314. *Id.*

315. *Id.*

316. *Id.* at 25–26.

317. *Id.*

318. FDA, POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (Dec. 27, 2016), https://www.fda.gov/media/95862/download [https://perma.cc/YT85-62W6].

E. The National Highway and Traffic Safety Administration (NHTSA)

Congress created NHTSA in 1970 in response to a crisis in driver safety.[319] Today, the spread of connected cars[320] threatens driver privacy (and thus, safety) in new ways due to invasive data collection and a lack of reliable cybersecurity. Conceptually, the category of privacy and safety problems relating to connected cars could be viewed as a special rolling member of the problems belonging to the IoT family, or it could be viewed as a special case of a more general problem of consumer choice and notice. Legally, however, car safety enjoys protection from NHTSA in addition to whatever coverage may flow from other agencies (not least the FTC),[321] so connected car safety is worth considering separately.

Connected cars have the ability to "access information via the Internet and gather, store, and transmit data for entertainment, performance, and safety purposes."[322] For example, connected cars collect consumers' precise location data, authentication data used for unlocking doors or logging into Facebook, biometric data, and "behavioral data (such as driving patterns, speed, acceleration, or vehicle stability), [and] personally identifiable information (such as a name, phone number, or username and password)."[323] In addition, when users pair their cell phones to a connected car, the car may gain the ability to copy personal information from the phone including call logs, contact lists, text and email messages, and in some cases deleted information.[324]

---

319. Highway Safety Act of 1970, Pub. L. No. 91-605 § 201(a), 84 Stat. 1739 (codified as amended at 49 U.S.C. § 105) (authorizing the Secretary of NHTSA to "carry out provisions of the National Traffic and Motor Vehicle Safety Act of 1966"). In the National Traffic and Motor Vehicle Safety Act of 1966, Pub. L. No. 89-563, 80 Stat. 718 (codified as amended in scattered sections of 49 U.S.C), Congress declared "that the purpose of this Act is to reduce traffic accidents and deaths and injuries to persons resulting from traffic accidents." In 1994, Congress repealed the 1996 Safety Act, but reenacted it as part of the National Highway Traffic Safety Administration Authorization Act, and recodified it in Title 49 U.S.C. §§ 301 et seq.

320. *See* FTC, CONNECTED CARS WORKSHOP 1 (Jan. 2018), https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf [https://perma.cc/B4ET-FZPX].

321. *See infra* text accompanying notes 332–34.

322. CONNECTED CARS WORKSHOP, *supra* note 320, at 1.

323. *FTC and NHTSA Navigate Privacy and Security Issues at "Connected Cars" Workshop*, WILMERHALE (July 5, 2017), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/ftc-and-nhtsa-navigate-privacy-and-security-issues-at-connected-cars-workshop [https://perma.cc/PXR9-5NDA].

324. Sam Biddle, *Your Car is Spying on You, and a CBP Contract Shows the Risks*, INTERCEPT (May 3, 20201) (noting ability of proprietary data-extraction software to extract data that can include "Recent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been" and in some cases deleted data, and data that allows software to "Identify known associates and establish communication patterns between them."), https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/ [https://perma.cc/GT9F-VPRB].

In short, connected cars collect reams of personal data. As with the IoT, consumers often are not aware of much of this collection, and even when consumers are aware of the collection, there is little they can do to prevent it without voiding their car's warranty. In addition to legal and potentially intrusive collection activities sanctioned by the cars' manufacturers, the existence of these data streams creates the risk that a malicious third party might acquire the data and endanger drivers' physical,[325] emotional,[326] and financial[327] well-being. Indeed, some connected cars create a risk that a hacker may take control of the vehicle, remotely threatening a driver's life.[328] Because connected cars threaten consumer privacy in each of these novel ways, NHTSA should recognize that its mission to keep drivers safe obligates it to develop standards that will ensure drivers are also safe from privacy and information security intrusions while in the car and on the road.

1. NHTSA Has Authority to Promulgate Rules Aimed at Protecting Privacy Related to Connected Cars

When it enacted the National Traffic and Motor Vehicle Safety Act of 1966 ("Safety Act of 1966"), Congress "determine[d] that it [was] necessary to establish motor vehicle safety standards for motor vehicles and equipment . . . ."[329] To do this, the Safety Act of 1966 directed the Secretary of Transportation to promulgate "[f]ederal motor vehicle safety standards,"[330] defined as "minimum standard[s] for motor vehicle performance, or motor vehicle equipment performance, which [are] practicable, which meet[] the need for motor vehicle safety and which provide[] objective criteria."[331] The Safety Act of 1966 defined "'motor vehicle safety" expansively:

> "Motor vehicle safety" means the performance of motor vehicles or motor vehicle equipment in such a manner that the public is protected

---

325. *Id.* (describing hackers' ability to remotely bring a vehicle to a stop on a busy highway); Eduard Kovacs, *Tesla Car Hacked Remotely From Drone via Zero-Click Exploit*, SECURITY WEEK (May 3, 2021), https://www.securityweek.com/tesla-car-hacked-remotely-drone-zero-click-exploit [https://perma.cc/UGF5-GEXK].

326. Edith Bevin, *Man Pleads Guilty to Stalking and Controlling Ex-Girlfriend's Car with His Computer*, ABC NEWS (last updated Nov. 6, 2019, 7:38 PM), https://www.abc.net.au/news/2019-11-06/ract-employee-pleads-guilty-to-using-app-to-stalk-ex-girlfriend/11678980 [https://perma.cc/R2MR-4E9V] (describing a woman's testimony that she was "'in shock and fear for [her life]'" when she realized her ex-boyfriend was tracking her movements and had control of her car").

327. *Cf. FTC and NHTSA Navigate Privacy and Security Issues at "Connected Cars" Workshop*, *supra* note 323 (describing how connected cars collect "biometric data (such as voice or fingerprint recognition)" and "personally identifiable information (such as a name, phone number, or username and password)").

328. *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [https://perma.cc/ZL5K-T6BB].

329. National Traffic and Motor Vehicle Safety Act of 1966, Pub. L. No. 89-563, 80 Stat. 718 (codified as amended in scattered sections of 49 U.S.C § 30302 et seq).

330. *Id.* 49 U.S.C. § 103(a) specifies that "[e]ach such Federal motor vehicle safety standard shall be practicable, shall meet the need for motor vehicle safety, and shall be stated in objective terms."

331. *Id.* § 102.

> against unreasonable risk of accidents occurring as a result of the design, construction or performance of motor vehicles and is also protected against unreasonable risk of death or injury to persons in the event accidents do occur, and *includes nonoperational safety of such vehicles*.[332]

Four years later, through the Highway Vehicle Safety Act of 1970, Congress created NHTSA and authorized the Secretary of Transportation to carry out the provisions of the Safety Act of 1966 through NHTSA.[333] Consequently, NHTSA became responsible for issuing safety standards.[334]

In 1994, Congress reenacted and recodified NHTSA's authority in the National Highway Traffic Safety Administration Authorization Act, but Congress left intact the broad grant of authority to regulate motor-vehicle safety. Congress again defined "[m]otor vehicle safety":

> [T]he performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes nonoperational safety of a motor vehicle.[335]

This inclusion of "nonoperational safety" in what otherwise is a focus on physical injuries from traffic accidents gives NHTSA authority to address injuries that might result from privacy risks associated with motor vehicles.

NHTSA understands that its authority relates to physical risks to drivers, passengers, and others arising from security risks to connected cars. Connected cars threaten drivers' physical safety if they allow third parties to take control of moving vehicles. "Because many of today's cars contain cellular connections and Bluetooth wireless technology," hackers can "gain remote access to someone's car just as they do to people's personal computers and take over the vehicle's basic functions, including control of its engine."[336] In an experiment, two researchers were able to take control of a Jeep Cherokee driving 70 miles per hour. They blasted the air conditioning, turned the music all the way up, turned on the windshield wipers, and cut the transmission, bringing the car to a complete stop on a highway.[337] When the Jeep was moving at low speeds, the experimenters had the ability to fully kill the

---

332. *Id.* (emphasis added).

333. Highway Safety Act of 1970, Pub. L. No. 91-605 §§ 201, 202(a), 84 Stat. 1739 (codified as amended at 49 U.S.C. §§ 30102 et seq.).

334. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *Regulations* (last visited March 13, 2021), https://www.nhtsa.gov/laws-regulations/fmvss [https://perma.cc/6ZFW-KDCF] ("NHTSA issues Federal Motor Vehicle Safety Standards (FMVSS) to implement laws from Congress. These regulations allow us to fulfill our mission to prevent and reduce vehicle crashes.").

335. 49 U.S.C. § 30102(a)(9).

336. John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y. TIMES (Mar. 9, 2011), https://www.nytimes.com/2011/03/10/business/10hack.html [https://perma.cc/995N-6SXJ].

337. Greenberg, *supra* note 328.

engine or disable the brakes.[338] The experiment highlighted the potential dangers of weak connected-car cybersecurity.

NHTSA recognizes that it has a role to play in the development of strong connected-car cybersecurity. Indeed, NHTSA acknowledges that "systems and components that govern safety must be protected from harmful attacks, unauthorized access, damage, or anything else that might interfere with safety functions."[339] To date, however, NHTSA has not issued cybersecurity regulations but instead has sought to encourage the industry to develop good cybersecurity practices through voluntary guidance.[340]

While NHTSA plays an active role in researching and encouraging protective cybersecurity practices,[341] it has shied away from using its "broad regulatory authority over the safety of passenger vehicles" to keep drivers safe from hackers.[342] Thus, "NHTSA agree[d]" with commentators arguing that, because "cybersecurity is a constantly evolving discipline and . . . best practices may need frequent updating, . . . NHTSA's cyber best practices should remain nonbinding and voluntary."[343] Although NHTSA should not constrain the development of cybersecurity by implementing overly specific guidelines, the seriousness of the safety interests threatened by weak cybersecurity means that NHTSA should embrace its rulemaking function to require reasonable minimum levels of cybersecurity, as other regulators do in areas such as banking and health.

Promisingly, NHTSA has indicated that it may take a more proactive approach to cybersecurity in the context of Automated Driving Systems ("ADS").[344]

---

338. *Id.*

339. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., VEHICLE CYBERSECURITY (last visited March 13, 2021), https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity.

340. *See, e.g.*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES (2016), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf [https://perma.cc/KT9Z-FCQQ].

341. *See, e.g.*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES: DRAFT 2020 UPDATE (2020), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf [https://perma.cc/NKB8-BZP5].

342. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *Request for Comments; Cybersecurity Best Practices for the Safety of Modern Vehicles*, 86 Fed. Reg. 2481, 2482 (Jan. 12, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-12/pdf/2021-00390.pdf [https://perma.cc/JT2H-MHBJ]; GOV'T ACCOUNTABILITY OFF., VEHICLE DATA PRIVACY: INDUSTRY AND FEDERAL EFFORTS UNDER WAY, BUT NHTSA NEEDS TO DEFINE ITS ROLE (July 2017), https://www.gao.gov/assets/gao-17-656.pdf [https://perma.cc/4L4L-UJJR].

343. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *Request for Comments; Cybersecurity Best Practices for the Safety of Modern Vehicles*, 86 Fed. Reg. 2481, 2482 (Jan. 12, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-12/pdf/2021-00390.pdf [https://perma.cc/JT2H-MHBJ].

344. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *Notice of Proposed Rulemaking; Framework for Automated Driving System Safety*, 85 Fed. Reg. 78058, 78064 (Dec. 3, 2020), https://www.govinfo.gov/content/pkg/FR-2020-12-03/pdf/2020-25930.pdf [https://perma.cc/X2UK-SQLQ].

In a request for comments on potential regulation, NHTSA stated that "addressing safety-related cybersecurity risks" was an "aspect[] that could impact the ability of an ADS to carry out its intended plans in a safe and reliable manner."[345]

Unfortunately, while NHTSA sees itself as having a role in cybersecurity, it has taken a much more limited view of its authority to make rules protecting privacy. NHTSA recently expressed the view "[t]hat its authorities under the Safety Act are limited to motor vehicle safety and, thus, do not authorize [NHTSA] to regulate areas such as general privacy and cybersecurity unrelated to safety."[346] And further, NHTSA's limited view of its authority to protect driver and passenger privacy is arguably in tension with the text of the National Highway Traffic Safety Administration Authorization Act of 1994, which, like the 1996 Act before it, includes authority to make rules regarding the "nonoperational safety" of motor vehicles.[347]

Fortunately, however, there is no real need to decide this question once one accepts, as *Privacy as Safety* tried to demonstrate, that in many cases privacy is, in and of itself, a safety issue.[348] Viewed in that light, many privacy issues become the very issues "related to safety" that NHTSA already views as falling within its jurisdiction.

Again, connected cars pose safety risks due to their increasing assault on driver and passenger privacy. Connected cars threaten drivers' safety by collecting large amounts of personal data. In addition to "precise location data" and other types of data related to performance and driving habits, connected cars collect "authentication data," "biometric data . . . , behavioral data . . . , [and] personally identifiable information . . . ."[349] Noting that "[c]ars have become the most sophisticated computers many of us own," a *Washington Post* reporter measured the amount of data that a car used its "hundreds of sensors" to collect: "On a recent drive, a 2017 Chevrolet collected my precise location. It stored my phone's ID and the people I called. It judged my acceleration and braking style, beaming back reports to its maker General Motors over an always-on Internet connection."[350] The amount and nature of personal data connected vehicles collect could threaten drivers' privacy and, consequently, drivers' safety.[351] To take just one example, detailed location data can put drivers at risk if it falls into the wrong hands.[352]

To help keep drivers safe, NHTSA should work to limit the increasing tendency of connected cars to collect and share information about riders. NHTSA

---

345. *Id.*
346. *Id.*
347. *See supra* text at note 330.
348. *See supra* Section I.A.
349. *FTC and NHTSA Navigate Privacy and Security Issues at "Connected Cars" Workshop*, *supra* note 323.
350. Geoffrey A. Fowler, *What Does Your Car Know About You? We Hacked a Chevy to Find Out*, WASH. POST (Dec. 17, 2019), https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/ [https://perma.cc/H3F3-VYDN].
351. Froomkin & Colangelo, *supra* note 1, at 163.
352. *Id.* at 164–75.

has acknowledged the extent of the problem by saying that connected cars "generate, use and may share a significant amount of vehicle data likely to be viewed by private citizens as sensitive and personal (for example, routes frequently travelled [sic] and precise addresses visited)."[353] But, rather than embrace its regulatory authority to address the safety issues resulting from weak data protection, NHTSA has taken a back seat to the FTC.[354] Arguing that the FTC "is the primary Federal agency responsible for protecting consumer privacy," NHTSA has confined itself to supporting the FTC's efforts[355] and issuing voluntary guidance.[356]

There is no reason why only one agency can concern itself with protecting privacy. Indeed, if privacy is conceptualized as a frequently necessary condition for safety, then the suggestion that only one agency can or should regulate in that domain is absurd. In 2017, the Government Accountability Office ("GAO") found that, despite NHTSA's "broad authority over the safety of passenger vehicles and consider[ation of] the privacy effects and implications of its regulations and guidance," "NHTSA has not clearly defined its roles and responsibilities as they relate to the privacy of vehicle data."[357] NHTSA concurred with the GAO's finding that NHTSA should "define, document, and externally communicate its roles and responsibilities related to the privacy of data generated by and collected from vehicles";[358] however, NHTSA has yet to embrace the broad role it should play in protecting drivers from privacy threats.

2. Examples of NHTSA Rules that Would Protect Privacy (and Strengthen Cybersecurity)

NHTSA should embrace its mandate of protecting drivers from the growing threats to their safety by implementing regulation aimed at bolstering cybersecurity and protecting data collected by connected cars. As a starting point, NHTSA could make many of its cybersecurity suggestions[359] into mandatory requirements. NHTSA's recently released update to its cybersecurity guidelines

353. *Vehicle Data Privacy*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. (last visited March 13, 2021), https://www.nhtsa.gov/technology-innovation/vehicle-data-privacy [https://perma.cc/HFB4-UQ6W].

354. *Id.*

355. *Id.* ("The FTC and NHTSA staff meet, coordinate, collaborate and communicate frequently on privacy issues related to motor vehicles, including those involving new technologies such as connected and automated safety systems.").

356. *See generally* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., AUTOMATED DRIVING SYSTEMS 2.0: A VISION FOR SAFETY (Sept. 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf [https://perma.cc/YQ28-X4GJ].

357. GOV'T ACCOUNTABILITY OFF., VEHICLE DATA PRIVACY: INDUSTRY AND FEDERAL EFFORTS UNDER WAY, BUT NHTSA NEEDS TO DEFINE ITS ROLE (July 2017), https://www.gao.gov/assets/gao-17-656.pdf [https://perma.cc/4L46-2WYH].

358. *Id.*

359. CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES: DRAFT 2020 UPDATE, *supra* note 341.

"aligned with two . . . European Union automotive cybersecurity regulations, which are binding."[360]

Specifically, NHTSA could require that connected-car developers "[e]nabl[e] an independent voice for vehicle cybersecurity-related considerations within the vehicle safety design process" by requiring that an outside auditor test cybersecurity risks and provide feedback.[361] NHTSA could also require manufacturers to issue cybersecurity reports documenting their own testing and risk assessment related to cybersecurity.[362] To help facilitate general management of cybersecurity and effective creation of cybersecurity reports, NHTSA could require connected-car manufacturers to "carry[] out organizational and product cybersecurity audits annually."[363]

In addition to building robust cybersecurity throughout the development process, NHTSA could mandate that connected-car manufacturers be prepared to mitigate the damage of cybersecurity breaches as they arise. NHTSA could require "[a] documented incident response plan" that sets out proper procedures for mitigating privacy breaches that do occur.[364] The plans could include procedures for quickly and effectively addressing vulnerabilities as they manifest.[365]

NHTSA could take steps aimed at the protection of personal data collected by connected cars.[366] As we suggest for the FTC's regulation of the IoT,[367] NHTSA

---

360. *Automotive Cybersecurity: Major Changes Underway*, EMBEDDED COMPUTING DESIGN (Jan. 15, 2021), https://www.embeddedcomputing.com/application/automotive/vehicle-networking/automotive-cybersecurity-major-changes-underway [https://perma.cc/J6KE-UHFC]; UN ECON. & SOC. COUNCIL, UN REGULATION ON UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARD TO CYBER SECURITY AND OF THEIR CYBERSECURITY MANAGEMENT SYSTEMS (June 23, 2020), https://unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf [https://perma.cc/4XMZ-H7MH]; UN ECON. & SOC. COUNCIL, PROPOSAL FOR A NEW UN REGULATION ON UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARDS TO SOFTWARE UPDATE AND SOFTWARE UPDATES MANAGEMENT SYSTEM (June 23, 2020), https://dig.watch/resource/proposal-new-un-regulation-uniform-provisions-concerning-approval-vehicles-regard [https://perma.cc/5S8A-JV4L]. Additionally, the update also included work from NIST, The International Standards Organization, and the Auto-ISAC. NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.1 (April 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018 [https://perma.cc/7NY2-33G3]; ISO/SAE 21434:2020 *Road Vehicles – Cybersecurity Engineering*, https://www.iso.org/standard/70918.html (last visited Nov. 16, 2022) [https://perma.cc/E74C-HTHU]; Auto-ISAC, *Best Practice Guides*, https://automotiveisac.com/download-best-practices (last visited Sept. 19, 2022) [https://perma.cc/FV3S-SV5U].

361. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., CYBERSECURITY BEST PRACTICES FOR THE SAFETY OF MODERN VEHICLES: DRAFT 2020 UPDATE, *supra* note 341, at 4.

362. *Id.* at 7.

363. *Id.* at 11.

364. *Id.* at 9.

365. *Id.* at 10.

366. Some of the following suggestions correspond with steps the FTC could take in the general sphere of the IoT, of which connected cars are a large part. *See* CAREFUL CONNECTIONS: KEEPING THE INTERNET OF THINGS SECURE, *supra* note 220.

367. *See supra* Section II.B.

could require that connected cars encrypt data both on-board and in transit to limit a third party's ability to access the data.[368]

NHTSA could also require auto manufacturers to have clear, accessible privacy policies. A disclosure rule would respond to current practices in which, "[m]ost [car manufacturers] hide what they're collecting and sharing behind privacy policies written in the kind of language only a lawyer's mother could love."[369] To help drivers understand the amount of information they are potentially putting at risk by using a connected car, NHTSA could require that car manufacturers publish specific and clear summaries of their privacy policies. For example, the policies could contain a complete explanation of the types of data being collected, how long the data is stored, and which third parties have access to what types of data.[370]

Last, but not least, NHTSA could require that manufacturers of connected cars allow consumers to opt out of certain categories of data collection and clearly communicate this right to their customers.[371] It may be appropriate to require the sharing of some data collected by connected cars about the vehicle's performance to help manufacturers and mechanics make cars safer,[372] but in many cases that information could be stored on board in a "black box" rather than continually transmitted somewhere. Especially regarding personal information,[373] however, the heightened sensitivity (and low marginal value for keeping cars safe) of the information justifies giving consumers the option to forbid the carmakers from collecting and using it. Indeed, today some manufacturers allow consumers to opt out of certain connected services.[374]

---

368. *See* CAREFUL CONNECTIONS: KEEPING THE INTERNET OF THINGS SECURE, *supra* note 220.

369. Fowler, *supra* note 350.

370. *See, e.g.*, *FTC and NHTSA Navigate Privacy and Security Issues at "Connected Cars" Workshop*, *supra* note 323 (noting "[a] concern among privacy advocates . . . that the collection of behavioral data by insurance companies would be used to increase insurance rates") https://www.ftc.gov/system/files/documents/videos/connected-cars-privacy-security-issues-related-connected-automated-vehicles-part-1/ftc_connected_cars_transcript_segment_1.pdf [https://perma.cc/A4TK-6W55].

371. California gives residents the right to prevent firms from selling or disclosing their personal information for any reason. *See* California Consumer Privacy Act (CCPA), CAL. CIV. CODE § 1798.120 et seq. (West).

372. *See, e.g.*, *FTC and NHTSA Navigate Privacy and Security Issues at "Connected Cars" Workshop*, *supra* note 323 (noting "that data on malfunctioning engine parts would be essential to suppliers and safety engineers, which makes the decision to give consumers autonomy over this data more difficult").

373. *Id.* (describing how connected cars collect "biometric data (such as voice or fingerprint recognition)" and "personally identifiable information (such as a name, phone number, or username and password)").

374. *See, e.g.*, TOYOTA, *Privacy Notice* (Apr. 11, 2022), https://www.toyota.com/privacyvts/ [https://perma.cc/E7WA-KFK7].

F. The Federal Aviation Administration (FAA)

Congress established the FAA to protect people's safety by regulating aircraft.[375] Today, aircraft pose new risks to people's safety by creating novel privacy risks. Drones, which have grown increasingly popular,[376] give users an increased ability to engage in voyeurism,[377] stalking,[378] and harassment,[379] and to avoid detection while doing so. To keep people safe from aircraft-related privacy risks, the FAA should develop regulations limiting unauthorized drone surveillance.

1. The FAA Has Authority to Promulgate Rules Protecting Privacy

In 1938, Congress passed the Civil Aeronautics Act to create the Civil Aeronautics Authority ("CAA") and "promote the development and safety and to provide for the regulation of civil aeronautics."[380] The CAA defined an aircraft as "any contrivance now known or hereafter invented, used, or designed for navigation

---

375. Federal Aviation Act of 1958, Pub. L. 85-726, 72 Stat. 740 (1958) (codified as amended at 49 U.S.C.).

376. FED. AVIATION ADMIN., FAA AEROSPACE FORECAST: FISCAL YEARS 2020–2040, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2020-40_FAA_Aerospace_Forecast.pdf [https://perma.cc/TLZ8-STQ7].

377. *See* Kristen Thomasen, *Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation*, 16 CANADIAN J.L. & TECH. 307 (2018); Paighten Harkins, *Utah Man Convicted of Using Drone to Spy on People in Their Homes Gets Suspended Jail Sentence*, SALT LAKE TRIBUNE (Oct. 31, 2017), https://www.sltrib.com/news/2017/10/31/utah-man-convicted-of-using-drone-to-spy-on-people-in-their-homes-gets-suspended-jail-sentence/ [https://perma.cc/EJ7F-Y55X] (describing how a drone pilot was convicted after a man "saw a drone flying outside his bathroom window," "followed it as [it] flew away and found it in a nearby church parking lot," and "found footage of people in their homes").

378. *Drone Stalker Jailed for Spying on Ex-Girlfriend*, BBC (Nov. 20, 2020), https://www.bbc.com/news/uk-wales-55018682 [https://perma.cc/XD82-SZF2] (describing how an ex-boyfriend "repeatedly used a drone to watch where [his ex-girlfriend] lived," making her feel "'absolutely mortified, sick and intimidated'").

379. Alison Branley & Rebecca Armitage, *Perpetrators Using Drones to Stalk Victims in New Age of Technology Fuelled Harassment*, ABCNEWS (last updated Sept. 30, 2018), https://www.abc.net.au/news/2018-10-01/drones-used-to-stalk-women-in-new-age-of-harassment/10297906 [https://perma.cc/5WG4-2AYE]. In addition to private drone operators' abuses, the rise of drones has also raised serious questions about the government's ability to monitor private citizens for law enforcement purposes. Gregory McNeal, *Drones and Aerial Surveillance: Considerations for Legislatures*, BROOKINGS (2014), https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures/ [https://perma.cc/5NU6-QK75]. Constitutional law provides some protection against this type of privacy infringement, but the potential for government abuse of drone surveillance has inspired a robust discussion on the need for added protection. *See, e.g.*, Hillary B. Farber, *Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment*, 64 SYRACUSE L. REV. 1 (2014); Jennifer M. Bentley, Note, *Policing the Police: Balancing the Right to Privacy Against the Beneficial Use of Drone Technology*, 70 HASTINGS L.J. 249 (2018).

380. Civil Aeronautics Act of 1938, Pub. L. No. 75-706, 52 Stat. 973 (codified as amended in 49 U.S.C.). In doing so, Congress built off of its original entry into regulating airplanes with the Air Commerce Act of 1926, a law giving the Secretary of Commerce authority to regulate air travel. Air Commerce Act of 1926, Pub. L. No. 69-254, 44 Stat. 568 (codified as amended in scattered sections of 49 U.S.C.).

of or flight in the air," and it defined appliances as "instruments, equipment, apparatus, parts, appurtenances, or accessories of whatever description, which are used, or are capable of being or intended to be used, in the navigation, operation, or control of aircraft in flight."[381] In a declaration of policy, Congress noted that the CAA's regulation of aircraft should seek to "assure the highest degree of safety in" air travel.[382]

The Civil Aeronautics Act authorized the CAA to create "[r]easonable rules and regulations and minimum standards governing, in the interest of safety," "the inspection, servicing, and overhaul of aircraft . . . and appliances" as well as "other practices, methods, and procedure, as the [CAA] may find necessary to provide adequately for safety in air commerce."[383] Then, in the Federal Aviation Act of 1958, Congress transferred the CAA's safety-regulation mandate to a new agency, the FAA.[384]

The FAA understands its safety mandate as being primarily concerned with keeping airplanes and other airborne craft from crashing, both to protect the physical safety of passengers and anyone who might have the misfortune of having an aircraft, or aircraft part, land on them or their house.[385] To date, however, the FAA has generally resisted calls to understand its safety mandate to embrace privacy.[386] This is an error.

---

381. Civil Aeronautics Act of 1938 § 1(4), 1(26), Pub. L. No. 75-706, 52 Stat. 973, 977–78 (codified as amended in 49 U.S.C.). Regarding the operation of aircraft, it specifically noted that "[a]ny person who causes or authorizes the operation of aircraft, whether with or without the right of legal control (in the capacity of owner, lessee, or otherwise) of the aircraft, shall be deemed to be engaged in the operation of aircraft within the meaning of this Act." *Id.*

382. *Id.* § 2(b). It also noted that the Civil Aeronautics authority should seek "[t]he regulation of air commerce in such manner as to best promote its development and safety[.]" *Id.*

383. *Id.* § 601(a).

384. Federal Aviation Act of 1958 § 601, Pub. L. 85-726, 72 Stat. 740, 775 (codified as amended at 49 U.S.C. § 1304).

385. *See, e.g.*, FAA, Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72,438, 72,514 (Dec. 31, 2019) "In the 2016 Rule [Operation and Certification of Small Unmanned Aircraft Systems, 81 FR 42064], . . . the FAA noted that privacy concerns were beyond the scope of the FAA's mission to ensure safety and efficiency of aviation operations in the airspace of the United States . . . .").

386. *See, e.g.*, FAA, Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9552 (Feb. 23, 2015) ("The FAA also notes that privacy concerns have been raised about unmanned aircraft operations. Although these issues are beyond the scope of this rulemaking, . . . the Department [of Commerce] and FAA will participate in the multi-stakeholder engagement process led by the National Telecommunications and Information Administration (NTIA) to assist in this process regarding privacy, accountability, and transparency issues concerning commercial and private UAS use in the NAS. We also note that state law and other legal protections for individual privacy may provide recourse for a person whose privacy may be affected through another person's use of a UAS.").

To fulfill its mission of keeping people safe from aircraft-related threats, the FAA should address privacy threats associated with drones.[387] Drones are growing in popularity,[388] and drone operators are increasingly using drones as tools to harm others. In addition to the potential for physical harm,[389] drone operators (and possibly drone hackers)[390] can threaten people's safety through unauthorized surveillance.[391] Demonstrating the ability of drone operators to infringe on an individual's privacy, a reporter "simulated ordinary activities both downstairs and upstairs in a typical house. A drone was able to monitor him on both floors while hovering out of sight."[392]

---

387. Congress explicitly acknowledged that drones fall under the FAA's regulatory authority with the FAA Reauthorization Act of 2018, which required a "final rule on [drone] systems that will allow for civil operations of such systems in the national airspace system." FAA Reauthorization Act of 2018, Pub. L. 115–254, 132 Stat. 3187, 3287 (codified at 49 U.S.C.). Recently, concern about the sufficiency of drone regulation prompted a bill seeking to direct the FAA to engage more drone regulation. Drone Integration and Zoning Act, S. 21077, 117th Cong. (2021), https://www.lee.senate.gov/public/_cache/files/a5dd4109-0dcf-44be-8489-cf755634a5bd/diza-117th.pdf [https://perma.cc/ZWA9-USZH].

388. FAA, FAA AEROSPACE FORECAST: FISCAL YEARS 2020–2040, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2020-40_FAA_Aerospace_Forecast.pdf [https://perma.cc/E9AR-P64N] (forecasting recreational drone fleet will grow to around 1.48 million units by 2024 and that commercial drone sector to about 828,000 aircraft in 2024).

389. *See, e.g.*, Martin Weil, *Drone Crashes Into Virginia Bull Run Crowd*, WASH. POST (Aug. 26, 2013), https://www.washingtonpost.com/local/drone-crashes-into-virginia-bull-run-crowd/2013/08/26/424e0b9e-0e00-11e3-85b6-d27422650fd5_story.html [https://perma.cc/TR99-XKPL]; Lauren Botchan, *Drone Injured Woman's Eye at Las Vegas Casino July 4th Party, Lawsuit Says*, ABCNEWS (Aug. 23, 2018), https://abcnews.go.com/US/drone-injured-womans-eye-las-vegas-casino-july/story?id=57358410 [https://perma.cc/6U8E-AHEY]. The FAA has addressed these safety concerns by regulating the use of drones at night and over people. 14 C.F.R. 107 § 107.39 (prohibiting the "operat[ion of] a small unmanned aircraft over a human being unless" certain conditions are met); 14 C.F.R. 107 § 107.29 (prohibiting the operation of "a small unmanned aircraft system during night" unless certain conditions are met).

390. April Glaser, *The U.S. Government Showed Just How Easy It Is to Hack Drones Made by Parrot, DBPower and Cheerson*, Vox (Jan. 4, 2017, 5:07 PM), https://www.vox.com/2017/1/4/14062654/drones-hacking-security-ftc-parrot-dbpower-cheerson [https://perma.cc/73FT-8ZV7] (describing how FTC researchers were able to "take over the video feed" on three drones because "the data was . . . unencrypted" and "take control of the [drones'] flight path, as well as turn off the aircraft").

391. Patrick J. Kiger, *Think a Drone is Spying on You? Here's What to Do*, HOWSTUFFWORKS (Aug. 13, 2019), https://science.howstuffworks.com/drone-spying.htm [https://perma.cc/W5W9-PAUL] (describing how an Oregon woman "was sitting at her computer one night in March 2019 when she noticed an unusual light outside her kitchen window," which she identified as belonging to a drone); Joe Pruski, *Drone Ace Has Day in Court*, DEFOREST TIMES-TRIBUNE (Oct. 9, 2015), https://www.hngnews.com/deforest_times/news/local/article_47b07034-6e90-11e5-860e-e7a77ccd08e7.html [https://perma.cc/9CL8-H5ZN] (violation of ordinance prohibiting "use [of] a drone to observe a person in a place where that person should have a reasonable expectation of privacy").

392. Jeff Rossen & Lindsey Bomnin, *Peeping Drones Could Be Spying on You in Your Own Home*, TODAY (May 9, 2018, 7:42 AM), https://www.today.com/money/peeping-drones-could-be-spying-you-your-own-home-t128590 [https://perma.cc/7YGB-A4CY].

The same monitoring capabilities demonstrated in that experiment have been abused by drone operators engaged in voyeurism, stalking, and harassment. In a real-world example, a drone operator was convicted of voyeurism after a neighbor, who spotted the operator's drone "flying outside his bathroom window," tracked it down and discovered that "the drone's SD card [had] footage of people in their homes."[393] Other instances of abuse involve violent ex-partners using drones to intimidate and monitor victims.[394] Unfortunately, the FAA has failed to address these serious drone-related privacy concerns.[395]

When the FAA announced a rulemaking about establishing a drone-regulation system, the Electronic Privacy Information Center ("EPIC") filed a petition advocating that the FAA "assess the privacy problems associated with the highly intrusive nature of drone aircraft, and the ability of operators to gain access to private areas and to track individuals over large distances."[396] But the FAA responded by characterizing privacy issues as "not an immediate safety concern"[397] and stating, in the drone regulation's Notice of Proposed Rulemaking, that privacy concerns were "beyond the scope of this rulemaking."[398] Rather than dismissing the serious threat to privacy posed by drone activity, the FAA should acknowledge these concerns as within its mission to keep people safe from aircraft.

---

393. Paighten Harkins, *supra* note 377.

394. *Drone Stalker Jailed for Spying on Ex-Girlfriend*, *supra* note 378, (describing an ex-partner's use of a drone to carry out "behavior intended to cause maximum fear and distress"). *See also* Branley & Armitage, *supra* note 379.

395. Jeramie D. Scott, *Drone Surveillance: The FAA's Obligation to Respond to the Privacy Risks*, 44 FORDHAM URB. L.J. 767, 774 (2017) ("Despite the many statements by the FAA regarding the importance of addressing the privacy implications of drones, when it came time to actually address privacy in the small drone rulemaking, the FAA shied away from the subject."); Jennifer Urban, *What Is the Eye in the Sky Actually Looking at and Who Is Controlling It? An international Comparative Analysis on How to Fill the Cybersecurity and Privacy Gaps to Strengthen Existing U.S. Drone Laws*, 70 FED. COMM. L.J. 1, 10 (2018) (FAA's drone regulations do "not provide enough clarification on how the issues of privacy and cybersecurity with drones should be handled"). Instead, the FAA has limited its drone regulation to addressing physical threats. *See* 14 C.F.R. 107. *See also* FED. AVIATION ADMIN., *Register Your Drone* (last updated Dec. 2, 2020, 11:29 AM EST), https://www.faa.gov/uas/getting_started/register_drone/ [https://perma.cc/ZJT6-Q22B].

396. Petition from the Epic Advisory Board, EPIC, to Michael P. Huerta, Acting Administrator, FAA (Feb. 24, 2012), https://epic.org/apa/lawsuit/EPIC-FAA-Drone-Petition-March-8-2012.pdf [https://perma.cc/ANM3-4WAL].

397. Letter from Lirio Liu, FAA, to Marc Rotenbug, EPIC Executive Director, and Amie Stepanovich, EPIC National Security Counsel (Nov. 26, 2014), https://epic.org/privacy/drones/FAA-Privacy-Rulemaking-Letter.pdf [https://perma.cc/D3SV-5GG9].

398. FAA, Notice of Proposed Rulemaking; Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9552 (Feb. 23, 2015), https://www.govinfo.gov/content/pkg/FR-2015-02-23/pdf/2015-03544.pdf [https://perma.cc/S9DZ-JRBD]. EPIC subsequently sued the FAA for its failure to include privacy concerns in its regulations, but the D.C. Circuit dismissed the suit for lack of standing. Elec. Priv. Info. Ctr. v. FAA, 892 F.3d 1249, 1251 (D.C. Cir. 2018).

2. Examples of FAA Rules That Would Protect Privacy

Because failing to protect privacy is tantamount to failing to protect safety, the FAA should be using its regulatory powers to protect passengers against the privacy threats posed by drones.[399] Specifically, the FAA could use its regulatory authority to create "a uniform regulatory scheme . . . that addresses the most imminent dangers of this technology such as trespass, nuisance, stalking, and voyeurism."[400] It could, for example, implement a blanket prohibition against low-altitude "aerial surveillance" of private property without consent.[401] It could also ban unauthorized flight over private property at low altitudes without consent[402] and prohibit drone users from "following an individual's movements with a drone."[403]

As we explained in *Privacy as Safety*, the FAA could also issue regulations aimed at reducing uncertainty about drones, generally:[404]

> A person confronted with a robotic trespasser, a robot that might be a spy, or a property-damaging robot, will in many cases have genuine and understandable doubts about the robot's capabilities and intentions. When, as a result of this uncertainty, a person assumes the worst about what the robot is doing or is going to do, her understandable lack of information about what the robot is capable of will–under some circumstances–provide a basis for a legal judgment that her belief was, in law, reasonable. Ordinarily, when confronted with new technologies, people fear them. When a technology is experimental or even just new, the social expectations needed to define a reasonable standard of care do not exist. As the use of the technology is abnormal, the risk is high that courts will find, or allow juries to find, that it is reasonable for people or even animals to be afraid of the technology. Because negligence is often measured against customary behavior, and new technology involves a departure from custom, one would expect that robots, at least for a while, will be reasonably held to appear to pose greater threats than they actually do. At least for the near future, so long as the public remains unfamiliar with, and potentially uncomfortable around, robots, judges and juries will likely find–and would be justified in finding–that a heightened level of caution and suspicion was "reasonable." Seeing fear and caution as reasonable will thus tend to push judges and juries

399. Drone users do have a role to play in protecting privacy, and thus safety. *See* NAT'L TELECOMMS. & INFO. ADMIN., *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability* (May 19, 2016), https://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf [https://perma.cc/J5TK-HPUF].

400. Alexandria Tomanelli, *A Drone's Eye View: Why and How the Federal Aviation Administration Should Regulate Hobbyist Drone Use*, 34 TOURO L. REV. 867, 871 (2018).

401. *Id.* at 897.

402. *See* Froomkin & Colangelo, *supra* note 4, at 55–56 (proposing a national rule re "vertical curtilage" or minimum navigable height).

403. Toban Platt, *The Drone Wars: The Need for Federal Protection of Individual Privacy*, 13 WASH. J.L. TECH. & ARTS 27, 46 (2017).

404. Froomkin & Colangelo, *supra* note 1, at 57–67.

> towards accepting a more muscular form of self-defense than society as a whole might decide to find reasonable once robots have become domesticated and commonplace–and it is likely to be a higher level than robot owners and operators would like.[405]

To reduce the uncertainty caused by drone overflights, trespasses, and the resulting safety risks—such as crashes and persons shooting down drones perceived to pose a threat—the FAA could, among other things, prohibit armed drones[406] and require drones that carry cameras or other data-gathering equipment to bear special markings or running lights to warn people being overflown of the drone's capabilities.[407] The FAA already requires that most drones weighing more than 250 grams be registered, which should allow injured parties to identify the owner if they can capture the drone.[408]

And starting in September 2022, the FAA requires most drone manufacturers to include in their products remote-identification capabilities that provide the identity, location, altitude, and velocity of the drone, as well as its control station or take-off location—but only to law enforcement, not the public.[409] Drone pilots themselves will need to ensure that their drone either contains built-in remote-identification capabilities or is equipped with a separate module that broadcasts the same information. The third option for drone pilots is to fly only within FAA-recognized identification areas (FRIAs) that are maintained by community organizations or educational institutions. But while the FAA continues to act in the safety arena, here by working to ensure accountability for drone harms, it is still ignoring the privacy impacts attendant to drone use.

G. The Occupational Safety and Health Administration (OSHA)

Congress created OSHA to ensure that workplaces are safe from both physical and intangible threats to worker safety.[410] To this end, OSHA develops standards "reasonably necessary or appropriate to provide safe or healthful employment and places of employment."[411] But the amount of data that employers can collect at the workplace,[412] paired with the lack of limitations on the use of

---

405. *Id.* at 57–58 (internal footnotes omitted).

406. *Id.* at 58–59.

406. *Id.* at 59–64.

408. FAA, Small Unmanned Aircraft Systems, 14 CFR part 107.

409. FAA, Remote Identification of Unmanned Aircraft, 14 CFR Parts 1, 11, 47, 48, 89, 91, and 107; FED. AVIATION ADMIN., Remote ID for Industry and Standards Bodies, https://www.faa.gov/uas/getting_started/remote_id/industry [https://perma.cc/J5N4-YVS8].

410. Occupational Safety and Health Act of 1970, Pub. L. No. 91-956, 84 Stat. 1590 (codified as amended at 29 U.S.C. §§ 651–678).

411. *Id.*; *see also* OSHA, *Law and Regulations* (last visited March 14, 2021), https://www.osha.gov/laws-regs [https://perma.cc/ASH4-JLKL] ("OSHA's mission is to ensure that employees work in a safe and healthful environment by setting and enforcing standards . . . .").

412. Meera Jagannathan, *Your Employer Has More Confidential Data on Your Than Amazon, Apple or Facebook*, MARKETWATCH (Aug. 4, 2019, 11:06 AM), https://www.marketwatch.com/story/your-employer-is-tracking-your-every-move-is-it-too-late-to-do-anything-about-it-2019-07-24 [https://perma.cc/YVV9-YEZ4].

workplace data,[413] threatens employee safety by posing risks to employee privacy. Employers have the capability to watch and listen to their employees through their laptops and mobile devices,[414] amassing vast amounts of employee data.[415] Because many employees lack the necessary awareness and control over the information-collection process,[416] or—especially in employment-at-will workplaces—lack the power to protest even if they do understand what is happening, OSHA should step in and support employee safety by placing reasonable restrictions on employers' power to collect and use employee data. Safe employment requires an environment that does not unreasonably threaten employee privacy.[417]

1. OSHA Has Authority to Make Rules Protecting Employee Privacy

Congress passed the Occupational Safety and Health Act of 1970 to "assure so far as possible every working man and woman in the Nation safe and healthful working conditions."[418] It established OSHA to implement this goal by promulgating enforceable standards.[419] OSHA *must* promulgate "any national consensus standard, and any established Federal standard, unless [the Secretary] determines that the promulgation of such standard would not result in improved safety or health," and it *may* promulgate any rule the Secretary determines would serve the objectives of the Occupational Health and Safety Act of 1970.[420] The standards were meant to "prescribe suitable protective equipment and control or technological procedures to be used" to keep workers safe.[421]

Twenty years ago, while issuing a final rule related to injury-reporting requirements, OSHA noted that the Occupational Safety and Health Act of 1970 "is concerned with both physical and mental injuries and illnesses, and in fact refers to 'psychological factors' in the statement of Congressional purpose."[422] OSHA's

---

413. *See* Steven Hill, *Employers are Spying on Remote Workers in Their Homes*, IN THESE TIMES (Sept. 23, 2020), https://inthesetimes.com/article/digital-surveillance-remote-workers-home-covid-pandemic-employers-control [https://perma.cc/64PN-EQ4C] ("Online surveillance of employees may seem invasive and creepy, but it is a legal practice in the United States . . . . Current laws are vastly outdated, as they are based on the Electronic Communications Privacy Act of 1986, when the primary form of electronic communication was the telephone.").

414. Aigerim Berzinya, *16 Worst and Most Extreme Ways Employers are Spying on Their People*, TURTLER (Nov. 27, 2020), https://turtler.io/news/16-worst-and-most-extreme-ways-employers-are-spying-on-their-people [https://perma.cc/UP9R-VDNE].

415. Jagannathan, *supra* note 412.

416. *Id.* (noting that "it can be difficult for employees to detect many types of surveillance on company-provided devices"); Hill, *supra* note 413 (describing an employee monitoring program that "can be secretly installed on workers' computers").

417. *See* Froomkin & Colangelo, *supra* note 1, at 163.

418. Occupational Safety and Health Act of 1970, *supra* note 410.

419. OSHA also has the authorization to enforce its standards and inspect workplaces to ensure compliance. *Id.*

420. *Id.*

421. *Id*.

422. OSHA, Final Rule; Occupational Injury and Illness Recording and Reporting Requirements, 66 Fed. Reg. 5916, 5953 (Jan. 19, 2001), https://www.govinfo.gov/content/pkg/FR-2001-01-19/pdf/01-725.pdf [https://perma.cc/E55F-QRR7].

mission, in its own view, thus encompasses protecting workers from both physical and psychological threats—and there is no reason why threats resulting from lack of privacy in the workplace should be excluded from this mission.

Employers collect vast amounts of employee data. Now, with more work being done at home, this collection often extends not just to the domicile but to family members and other domestic visitors. Modern employee-monitoring programs installed on computers and phones (sometimes without employee awareness) allow employers to monitor much more than simple work habits.[423] For example, a 2018 survey of over 200 large companies revealed that over half of the companies used "'some type of nontraditional monitoring techniques,' which included tactics like analysis of email and social-media messages, and collection of biometric data."[424] In addition to programs that track "a worker's mouse movements, keyboard strokes, webpages visited, email, file transfers[,] applications used," and "location," some types of employee-monitoring software "[d]ownload[] videos of employees' screens and use[] a computer's webcam, which can take a picture of the employee every 10 minutes."[425] Since COVID-19 drove many people to work from home, this practice results in frequent videos or snapshots of employees' homes.[426] The ability of these programs to monitor employees is particularly concerning because some of the programs can "be installed (even remotely via company servers) invisibly" and offer "a stealth monitoring feature" that monitors employees without their knowledge.[427]

Employee privacy is further threatened by the lack of legal constraints or effective federal privacy policies limiting employers' ability to collect or use employee data.[428] The lack of federal laws against workplace surveillance gives employers "'carte blanche to install any surveillance monitoring systems in the

423. Berzinya, *supra* note 414.
424. Jagannathan, *supra* note 412.
425. Hill, *supra* note 413.
426. *Id.*
427. Berzinya, *supra* note 414.
428. Although some of the tactics that employers use to monitor employees could fall under the Electronic Communications Privacy Act's ("ECPA") broad prohibition on intercepting electronic communication without consent, the ordinary course of business exception limits the ECPA's effect on employers. 18 U.S.C. § 2510(5)(a). *See also* Eric Bosset & Hannah Lepow, *Key Issues in Electronic Communications Privacy Act (ECPA) Litigation*, PRACTICAL L. (2020), https://www.cov.com/-/media/files/corporate/publications/2020/06/key-issues-in-electronic-communications-privacy-act-ecpa-litigation.pdf [https://perma.cc/B4FP-CECR] (discussing how the ECPA "exempts from liability the interception of communications" that were "furnished to a subscriber (or user) in the ordinary course of its business and that the subscriber (or user) used in the ordinary course of its business.").

workplace or on work equipment.'"[429] Although there are some exceptions,[430] most state laws fail to give employees privacy protection in the workplace.[431]

The lack of legal constraints on the collection and use of data leaves privacy policies as the only tool against abuse of employee information, but many workplace privacy policies fail to give employees adequate control over their information. A report based on "surveys of 1,400 C-level executives and 10,000 workers across 13 industries" found that "[o]nly 32 percent of employees say they have consented to employer use of workplace data, and 56 percent of business leaders say their companies do not ask for consent."[432] Another concerning figure is the finding that "[j]ust about half of the C-suite executives (49%) say they will use the workplace data as they see fit, with no additional responsibility measures; only 31 percent say employee concerns are holding them back . . . ."[433] Despite the importance of allowing employees to play a meaningful role in the control of their information, "[o]nly 29 percent of business leaders say they have co-created workplace data policies."[434]

OSHA could use its authority to keep workers safe and help remedy the existing threat of misuse of employee data. In 2019, "[m]ore than two thirds (70%) of business leaders globally said they [were] 'not very confident' that they [were] using new sources of workplace data in a 'highly responsible' way."[435] Much employee data is routinely shared with third parties to outsource administrative tasks.[436] For example, "thousands of human resource departments around the country" gave sensitive employee information to Equifax as "an easy way to

---

429. Jagannathan, *supra* note 412.

430. *See, e.g.*, Benjamin Ebbink & Usama Kahf, *California's Groundbreaking Privacy Law Amended: What Do Employers Need To Know?*, FISHERPHILLIPS (Oct. 12, 2019), https://www.fisherphillips.com/news-insights/employment-privacy-blog/california-s-groundbreaking-privacy-law-amended-what-do-employers-need-to-know.html [https://perma.cc/D2XT-2V2V]; Eric Rosenbaum, *Companies are Collecting More Data on Employees, and Not at All Confident They are Doing it Responsibly*, CNBC (last updated Jan. 23, 2019, 12:56 PM), https://www.cnbc.com/2019/01/23/the-next-big-negotiation-with-a-boss-access-to-your-personal-data.html [https://perma.cc/WYY2-VG2J] (noting that, in 2019, there [were] only two states, Delaware and Connecticut, where there [was] a law overseeing workplace collection of data").

431. *See* Hill, *supra* note 413 (noting that "[i]ndividual state laws vary over whether companies must inform workers that they're using tracking software, but in reality 'when you're on your office computer, you have no privacy at all'").

432. *More Responsible Use of Workforce Data Required to Strengthen Employee Trust and Unlock Growth, According to Accenture Report*, ACCENTURE (Jan. 21, 2019), https://newsroom.accenture.com/news/more-responsible-use-of-workforce-data-required-to-strengthen-employee-trust-and-unlock-growth-according-to-accenture-report.htm [https://perma.cc/M44L-JVQR]; Rosenbaum, *supra* note 430.

433. Rosenbaum, *supra* note 430.

434. However, "another 33 percent say they do plan to do so in the future." *Id.*

435. *Id.*

436. *See, e.g.*, Red Tape, *Exclusive: Your Employer May Share Your Salary, and Equifax Might Sell that Data*, NBC NEWS (Jan. 30, 2013, 4:44 AM), https://www.nbcnews.com/technolog/exclusive-your-employer-may-share-your-salary-equifax-might-sell-1B8173066 [https://perma.cc/3GA9-YPXJ].

outsource employment verification of former workers."[437] Equifax would then sell some of the information to third parties, including "debt collectors, financial service companies and other entities."[438] This example of how employers can use large amounts of employee information without employee knowledge or meaningful consent highlights the need for OSHA to step in to protect workers from privacy threats in the workplace.

2. Examples of OSHA Rules That Would Protect Privacy

To keep workers safe in an environment that collects massive amounts of sensitive data,[439] OSHA could impose limits on what sort of biometric and data surveillance employers can impose on employees. OSHA could also implement rules requiring employers to safeguard employee data and provide employees with transparency and control over how data is collected and used, as well as a right to contest and correct errors.

OSHA could require that employers surveilling their employees create structural policies that require a code of conduct, identification of executives responsible for ensuring the privacy and security of data, conformity to security standards, and regular audits by credentialled professionals checking how information is collected and stored.[440] An auditing requirement encourages corporations to devote more executive-level effort toward protecting employee information. Some commentators have noted that "[i]deally, a C-level executive would be accountable for ensuring that workplace data and technologies are used in a responsible and ethical way. But less than 20% of the companies captured in our survey have a C-level executive in charge of this today, although another 48% reported having plans to change that soon."[441]

OSHA could also require employers to give employees direct access to and control over employee information. This requirement could force employers to adopt procedures enabling an employee to request the following: (1) disclosure "of what personal information [an employer] has about the individual or what information [the employer] has shared"; (2) "deletion of the information"; and (3) "access to or a copy of some or all of the information."[442] An effective method of including employees in the process of collecting and using employee information

437. *Id.*

438. *Id.*

439. Berzinya, *supra* note 414.

440. *See* California Consumer Privacy Act (CCPA), *supra* note 39; *see also* Ebbink & Kahf, *supra* note 430 (stating that California businesses must "ensure they have implemented reasonable security measures, both physical and electronic, to safeguard the personal information of employees and job applicants").

441. Ellyn Shook et al., *How Companies Can Use Employee Data Responsibly*, HARV. BUS. REV. (Feb. 15, 2019), https://hbr.org/2019/02/how-companies-can-use-employee-data-responsibly [https://perma.cc/EF65-59XG].

442. This recommendation is based on California's requirements. Ebbink & Kahf, *supra* note 430.

"would be to create a single place where they can see, manage, and even delete the data their employer has collected about them."[443]

OSHA could also require external audits of how companies collect and store employee information. A system requiring companies to undergo an external audit may be a more effective means of holding them accountable for the way they collect and store employee information.[444]

To give employees a better understanding of how employee information is collected and used, OSHA could also require significant improvements in employee privacy policies. It could require that privacy policies be easily accessible and contain clear disclosures related to "the categories of personal information" collected by the employer and "the purposes for which the information will be used."[445] Ideally, workers would have rights to enforce privacy policies if they are violated, but liability rules of that sort may well exceed OSHA's authority.

CONCLUSION

This Article does three things. First, we redeem the promise made in *Privacy as Safety*[446] and demonstrate that recognizing that privacy often contributes to safety, and sometimes is necessary for it, has substantial implications for the ability of agencies with safety missions to regulate in ways that would greatly enhance personal privacy.

Second, we identify a wide variety of specific privacy-enhancing regulatory actions that six selected agencies with a consumer or safety orientation—the FTC, the CPSC, the FDA, NHTSA, the FAA, and OSHA—could each take under their existing statutory authority. The regulatory actions we identify above constitute only a sample of what might be considered low-hanging fruit. While the process of agency rulemaking is neither costless nor necessarily swift, we believe that each of the examples presented represents an action that would amply justify the regulatory effort.

Our third point follows from the second: our examples demonstrate that the United States' sectoral approach to privacy law offers considerable untapped potential for improvements to personal privacy, even without any new legislation. By making this showing, we do not mean to dispute the idea that even greater progress toward protection of privacy might be achieved by the passage of general or omnibus federal privacy legislation on the model of the European Union's GDPR. Rather, we seek only to show that important and tangible progress can be

---

443. Shook et al., *supra* note 441 (discussing an example of a company that "maintains an internal site called MyCareer that allows workers to keep and update their own career data, and even challenge any incorrect or incomplete inputs").

444. *Cf.* Ebbink & Kahf, *supra* note 430 ("It is a best practice to undergo an external security audit by an independent security consulting firm, not by your internal or outsourced IT vendor.").

445. This recommendation too is based on a requirement under California law. *Id*.

446. *See supra* Section I.A.

accomplished while waiting (and waiting) for progress at the federal level or from all 50 states.[447]

In politics, there is always a risk that fixing parts of a large problem piecemeal undermines the case for wholesale reform by making the overall problem seem less dire. We acknowledge that danger. But given the many existing obstacles to a comprehensive privacy solution in the United States, not least a gridlocked Congress, that seems to be a risk worth taking.

447. *See supra* note 45.