2017

The Inadequate, Invaluable Fair Information Practices

Woodrow Hartzog
Boston University School of Law

THE INADEQUATE, INVALUABLE FAIR INFORMATION PRACTICES

WOODROW HARTZOG*

TABLE OF CONTENTS

INTRODUCTION

Privacy law is in a bit of a pickle thanks to our love of the Fair Information Practices ("FIPs"). The FIPs are the set of aspirational principles developed over the past fifty years used to model rules for responsible data practices. Thanks to the FIPs, data protection regimes around the world require those collecting and using personal information to be accountable, prudent, and transparent. They give data subjects control over their infor-

* Starnes Professor of Law, Samford University's Cumberland School of Law; Affiliate Scholar, Center for Internet and Society at Stanford Law School. The author would like to thank Danielle Citron, Ryan Calo, and Brannon Denning for their helpful comments, and Carmen Weite for her research assistance.

mation by bestowing rights of correction and deletion. While the FIPs have been remarkably useful, they have painted us into a corner.[1]

A sea change is afoot in the relationship between privacy and technology. FIPs-based regimes were relatively well-equipped for the first wave of personal computing. But automated technologies and exponentially greater amounts of data have pushed FIPs principles like data minimization, transparency, choice, and access to the limit. Advances in robotics, genetics, biometrics, and algorithmic decisionmaking are challenging the idea that rules meant to ensure fair aggregation of personal information in databases are sufficient. Control over information in databases isn't even the half of it anymore. The mass connectivity of the "Internet of Things" and near ubiquity of mobile devices make the security and surveillance risks presented by the isolated computer terminals and random CCTV cameras of the '80s and '90s seem quaint.

But we've come too far with the FIPs to turn back now. The FIPs model of privacy regulation has been adopted by nearly every country in the world that has decided to take data protection seriously.[2] Normatively, the FIPs have been with us so long that in many ways they have become synonymous with privacy. At this point, abandoning the FIPs is out of the

1. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 342 (Jane K. Winn ed., 2006); Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1218–19 (2013) (arguing that even updated versions of the FIPs fail to update the definition of personal data, exacerbate the problematic central role of consent, remain rooted on a linear approach to data processing, and problematically continue to view information as "residing" in a jurisdiction); *see also* DANIEL J. WEITZNER ET AL., COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY, MIT-CSAIL-TR-2007-034 TECHNICAL REPORT: INFORMATION ACCOUNTABILITY (2007); Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 131, 132–33 (Austin Sarat ed., 2015); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 499–500 (1995) ("[I]nstead of minimizing the manipulation of citizens and their thinking through unfettered flows of information, the private sector has established a 'smoke screen' that in effect enables subtle, yet significant, manipulation of citizens through hidden control of personal information."); Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 ISJLP 425, 489 (2011). *But see* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1670–71 (1999); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1; Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 745 ("I propose an approach to Internet privacy centered around fair information practices (FIPs), which are rules for the fair treatment of personal information."); Paula Bruening, *Rethink Privacy 2.0 and Fair Information Practice Principles: A Common Language for Privacy*, POLICY@INTEL (Oct. 19, 2014), http://blogs.intel.com/policy/2014/10/19/rethink-privacy-2-0-fair-information-practice-principles-common-language-privacy/.

2. *See, e.g.*, COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 12 (2006); GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES 6–7 (2014). *See generally* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION (2d ed. 2007).

question. Even tinkering with them requires true urgency and a good plan. But modern privacy problems require more than just the FIPs. Hence, the pickle.

The coming evolution of privacy risks presents an opportune moment to assess the state of the FIPs in the modern world and ask whether they are up to the task. This Essay is an attempt to identify the practical virtues and vices of the FIPs to help privacy law evolve while retaining traditional notions of data accountability. The thesis of this Essay is that while we cannot do without the FIPs, it is time for lawmakers to stake out new ground. The FIPs are necessary, but not sufficient. To make privacy law whole, the FIPs must be treated as one of several frameworks to protect our personal information.

My argument proceeds in three parts. I begin by analyzing why the FIPs have proven so resilient. These simple principles have come a long way from that report issued by the Advisory Committee on Automated Personal Data Systems in the Department of Health, Education and Welfare in 1973.[3] Now they are synonymous with data protection all over the world. Europe's insistence on adequate privacy laws for international data exchanges has ensured that the rest of the data-creating world will implement some version or aspect of the FIPs.[4]

In Part I, I argue that in many ways, this is good. The FIPs provide a common set of values, which is necessary as data flows from one country to another at the speed of light. The FIPs provide a benchmark for industry, advocates, and policymakers to analyze new technologies. Privacy as a general concept is vague and messy. But the FIPs are a little more concrete. This clarity gives everyone a more useful litmus test for determining whether companies are being responsible with people's data. In short, the FIPs are invaluable for the modern world.

In Part II, I tackle the shortcomings of the FIPs. First, the FIPs have several blind spots. The FIPs are largely focused on data aggregation by industry. They do not contemplate peoples' vulnerabilities to each other on platforms like social media, peoples' susceptibility to manipulation, and peoples' helplessness to automated decisionmaking. New technologies and practices such as "big data" and artificial intelligence don't fit well with the FIPs, which were designed to address relatively simple data processing problems like unauthorized disclosure and inaccurate data. Some of the FIPs, like data minimization, are seen as anathema by those that see the

3. U.S. DEP'T OF HEALTH, EDUC. & WELFARE, No. (OS)73-94, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973) [hereinafter RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS].

4. *See* GREENLEAF, *supra* note 2, at 7; Christopher Wolf, *Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*, 43 WASH. U. J.L. & POL'Y 227, 231 (2013).

promise of big data.[5] Advocates of big data argue that the true potential of these new technologies will be revealed when there is more information, not less. Meanwhile, problems like racial bias and discrimination in algorithmic systems and interposal privacy issues on social media are blind spots for the FIPs.[6] More are looming. Anthropomorphized robots, fMRIs that measure brain activity, and advances in genetics raise problems like susceptibility to things that look human, the inability to hide thoughts, and discrimination based on predictions of things that haven't even happened yet.[7] These problems are beyond the scope of the FIPs.

Next, I argue that the FIPs-regimes ignore the fact that data subjects have limited cognitive and practical resources to draw upon to ensure their data is protected. I call this the "bandwidth problem." Laws based on the FIPs like Europe's General Data Protection Regulation ("GDPR") and Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") ostensibly give people control over how their information is collected and processed.[8] But whether these FIPs-based laws provide sufficient protection is debatable.[9] Often they simply transfer the risk of privacy

5. Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 243–51 (2013) (noting the "big benefits" of Big Data in the areas of healthcare, mobile, smart grid information, traffic management, retail, fraudulent payments, and online data); Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 64 (2012) ("The uses of big data can be transformative, and the possible uses of the data can be difficult to anticipate at the time of initial collection."). *But see* Paul Ohm, *The Underwhelming Benefits of Big Data*, 161 U. PA. L. REV. ONLINE 339, 340 (2013) ("Big Data's touted benefits are often less significant than claimed and less necessary than assumed.").

6. *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677 (2016); James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1189 (2009) ("Even if Facebook were perfectly ethical and completely discreet, users would still create false profiles, snoop on each other, and struggle over the bounds of the private. For this reason, while reports dealing with privacy and other platforms often propose strong restrictions on data collection and transfer, the focus of reports on social-network-site privacy is appropriately elsewhere.").

7. *See* Ifeoma Ajunwa, *Genetic Data and Civil Rights*, 51 HARV. C.R.-C.L. L. REV. 75 (2016); Bradley A. Areheart, *GINA, Privacy, and Antisubordination*, 46 GA. L. REV. 705 (2012); M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 29 (2011) (arguing that drones may be the "jolt" that brings privacy law up to speed with advancing technology); Nita A. Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351 (2012); Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239 (2012); Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785 (2015); Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CAL. L. REV. CIR. 57, 57 (2013) (discussing the regulation of private and government drone use and surveying "potential axes" of how states may regulate drone use); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016); Jessica L. Roberts, *The Genetic Information Nondiscrimination Act as an Antidiscrimination Law*, 86 NOTRE DAME L. REV. 597 (2011); Hideyuki Matsumi, Privacy Law Scholars Conference Paper Workshop: Do I Have Privacy Rights Over Predictive Information? (May 6, 2016) (unpublished manuscript) (on file with author).

8. Council Regulation 2016/679, 2016 O.J. (L 119) 1; Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.).

9. *See* Cate, *supra* note 1, at 342 and accompanying text.

harm to the person whose information is being collected and used. This is because control simply does not scale. People have limited resources and time (what I call bandwidth) and have too many requests for "consent" for all of them to be meaningful.

Finally, I argue that the FIPs have ossified. While the ability of the FIPs to harmonize data protection regimes has many benefits, a commitment to harmony with other regimes makes significant change difficult. Even when entire regimes change, as with the GDPR, the fundamental framework is still built around the FIPs and control, with changes at the margins. Ossification would be fine if this version of the FIPs were all the world needed. But the myopia and bandwidth problems mean we need something more. In short, the FIPs are inadequate for the modern world.

In Part III, I propose a new path forward for privacy law. The best strategy might be to keep data accountability law rooted in the FIPs while incorporating new frameworks and principles. For example, competition policy is now more relevant than ever, as data-driven online industries are opaque, have incredible power over consumers, and impose high barriers to entry.[10] Civil rights and antidiscrimination laws should be brought to bear on data use. Lawmakers should focus more on the design of consumer technologies. How something is built affects how it is perceived or used. The design of consumer technologies can be used to frustrate fair data practices like control and transparency, or it can circumvent them and render data protection laws formulistic.

The FIPs are not focused on design. They focus on de-contextualized goals, like "openness" and "data quality." Phrases like "security safeguards" and "means of openness" in the FIPs show where design might complement privacy policy. Passwords and online portals are security and transparency solutions, respectively, that leverage design. But because the FIPs do not give any specific technology mandates or design guidance, and because there is no mandate to examine how people actually perceive and interact with consumer technologies, privacy law has largely glossed over design. So, while the FIPs are quite useful for problems with data and databases, we must dig deeper.

I. THE FIPS ARE INVALUABLE

The FIPs have come a long way from their humble origins. In the 1970s, proto-versions of the FIPs started percolating in some of the earliest data privacy laws and government reports around the world. The FIPs were first labeled as such in a 1973 report issued by the Advisory Committee on Automated Personal Data Systems for the Secretary of the U.S. Department

10. *See* MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY (2016).

of Health, Education & Welfare (HEW).[11] The report, entitled *Records, Computers and the Rights of Citizens*, proposed the FIPs as a set of principles for protecting the privacy of personal data in recordkeeping systems in response to growing privacy concerns over computerized databases maintained in both the public and private sector.[12] The HEW report recommended some basic fair information principles that had shown up in scattered legislation and reports around the world, including transparency, use limitation, access and correction, data quality, and security.[13] These principles were the foundation for the U.S. Privacy Act of 1974, which passed the year after the report came out.[14]

While the HEW report and a few privacy laws in Europe embraced some notion of accountability and transparency for data practices, the FIPs did not really catch fire until they were officially adopted in 1980 by the Organisation for Economic Co-operation and Development ("OECD") in its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and in 1981 by the Council of Europe in the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[15]

The OECD's version of the FIPs implore data collecting entities to:

- Limit the amount of personal data they collect, and collect personal data with the knowledge or consent of the data subject (the "Collection Limitation Principle");
- Ensure that the data collected is relevant to the purposes for which it will be used and is "accurate, complete, and up-to-date" (the "Data Quality Principle");
- Specify the purposes for which data is collected (the "Purpose Specification Principle");
- Obtain consent to use and disclose personal data for purposes other than those specified at the time of collection (the "Use Limitation Principle");

11. Robert Gellman, Fair Information Practices: A Basic History 2 (Dec. 22, 2016) (unpublished manuscript), http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

12. *Id.*

13. RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, *supra* note 3; *see also* Katrine Evans, *Where in the World Is My Information? Giving People Access to Their Data*, 12 IEEE SECURITY & PRIVACY 78, 78–79 (2014); Robert Gellman, *Willis Ware's Lasting Contribution to Privacy: Fair Information Practices*, 12 IEEE SECURITY & PRIVACY 51, 51–52 (2014); Deirdre K. Mulligan, *The Enduring Importance of Transparency*, 12 IEEE SECURITY & PRIVACY 61, 62 (2014).

14. 5 U.S.C. § 552(a) (2012); *see also* Cate, *supra* note 1, at 346–47.

15. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (1980) [hereinafter *OECD Guidelines*], http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; Eur. Consult. Ass., *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS No. 108 (1981).

- Take "reasonable security safeguards" to protect data (the "Security Safeguards Principle");
- Be transparent about their data collection practices and policies (the "Openness Principle");
- Allow individuals to access the data collected from them, to challenge the data, and to have inaccurate data erased, rectified, completed, or amended (the "Individual Participation Principle"); and
- Be accountable for complying with the principles (the "Accountability Principle").[16]

Although neither the Council of Europe Convention or the OECD Guidelines used the term "fair information practices," both of them relied upon the FIPs to create their guidelines. The OECD Privacy Guidelines are now the most commonly cited version of the FIPs.[17] The OECD claimed that the FIPs were created to "represent a consensus on basic principles which can be built into existing national legislation" and to "serve as a basis for legislation in those countries which do not yet have it."[18] There is no question that the guidelines were successful. After the OECD guidelines, it was off to the races for the FIPs. There are now more than 100 countries with data privacy laws and most of them are built upon most or all of the minimum fair information practices specified by the OECD.[19] Before I discuss the FIPs' shortcomings, in this Part I'll focus on their significant benefits, including giving the world a common language of privacy, being malleable and severable, and establishing a reference point for analyzing new technologies and data practices.

A. A Common Language of Privacy

One of the most amazing things about a concept as diverse and squishy as privacy is that there is some consensus on the basic rules involving personal data. Privacy is an inherently contextual, culturally dependent concept. Lawmakers often create problems when they attempt to impose one country or culture's privacy sensibilities across cultures and individuals. Intel's Paula Bruening observed that even in light of this cultural sensitivi-

16. *OECD Guidelines*, *supra* note 15.

17. Gellman, *supra* note 11, at 8.

18. *OECD Guidelines*, *supra* note 15.

19. *See* GREENLEAF, *supra* note 2, at 52–58. Greenleaf also notes that in addition to the "minimum" or first generation FIPs issued by the OECD, a second generation of FIPs has arisen out of Europe, which incorporates that first generation of FIPs and adds substantive protections like data export restrictions, rights of deletion, sensitive data protection, automated processing controls, and direct marketing opt-outs. *Id.* at 55–56; *see also* Council Directive 95/46, art. 189, 1995 O.J. (L 281) 31 (EC); *Data Transfers Outside the EU*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm (last visited May 17, 2017).

ty, the "internationally recognized, fundamental principles of fair information practices continue to provide a common language about data protection and privacy that has served nations, regions, companies and individuals around the world, without demanding a departure from local privacy values."[20] Bruening also noted that when there is a perceived privacy failure, the FIPs can be used to measure compliance and as a means of enforcement.[21]

Indeed, the FIPs are the closest thing the world has to a universal privacy touchstone. Nearly every privacy regime in the world in some way has been shaped by the FIPs, which is surprising given the other possibilities. Recall the many different possible conceptions of privacy: control, secrecy, intimacy, dignity, autonomy, trust, the right to be let alone, limited access to the self, personhood, and more.[22] Data protection laws could revolve around any of them. Imagine more limited data protection regimes that only protect true secrets or more expansive ones that protect predictions and opinions in addition to "personally identifiable information."[23] Perhaps regimes could consider some privacy rights inalienable or mandate that data subjects protect themselves.[24] Or they might not bestow such responsibility and respect on the concept of "consent" and "control." But for better or worse, the dominant conceptualization of privacy in data protection regimes around the world is control over personal information.

While it might be tempting to chalk the lack of diversity in privacy law up to a paucity of imagination, the reason control won out is likely simple economics. The "control" conceptualization of privacy is built for globalization of the data trade. Users are given control when they are given *notice* of a company's information practices and they give *permission* to data processors to collect and use their information. Once that permission is granted, data can be collected, processed, leveraged, and shared accordingly. In theory, data subjects are happy. Data processors are happy. We all win and the data spigot keeps pouring. Though, as we will see, it has not really worked out that way.

The mass adoption of FIPs-based regimes facilitated the European Union's omnibus data protection legislation, which was built upon the FIPs

20. Bruening, *supra* note 1; *see also* Paula Bruening, *Fair Information Practice Principles: A Common Language for Privacy in a Diverse Data Environment*, POLICY@INTEL (Jan. 28, 2016), http://blogs.intel.com/policy/2016/01/28/blah-2/.

21. Bruening, *supra* note 1.

22. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1092, 1094 (2002).

23. Tene, *supra* note 1, at 1219 n.1; *see also id.* at 1219 ("[T]he second generation [of the FIPs] fails to update the definition of personal data, the fundamental building block of the [OECD] framework." (footnote omitted)).

24. For more thoughts on inalienable privacy rights, see ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011), Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71 (2016), Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845 (2013).

and prohibited data transfers to countries that lacked adequate data protection.[25] Countries seeking to collect and process data from E.U. citizens had great incentive to mold their own laws after the E.U.'s Data Directive (now GDPR), further entrenching FIPs-based regimes around the world.

The dominance of the FIPs now means that the European Union, Canada, Australia, and many Asian countries all speak substantially similar languages when it comes to data protection.[26] Even in "FIPs-lite" countries, the FIPs provide a starting point for finding common ground. For example, the FIPs contour U.S. privacy statutes like the Health Insurance Portability and Accountability Act[27] ("HIPAA") and the U.S. Federal Trade Commission's ("FTC") regulation of privacy, particularly through the FTC's authority to police unfair and deceptive trade practices.[28]

Having a common language of privacy across countries opens the door for remarkable diplomatic solutions for protecting privacy in the global digital economy. Such common ground allowed the United States and Europe to negotiate first the U.S.-E.U. Safe Harbor and then the E.U.-U.S. Privacy Shield to facilitate the transfer of personal data outside of the European Union.[29] A common language of privacy has also been critical in the creation of Asian-Pacific Economic Cooperation's ("APEC") cross-border privacy rules, which are designed to ensure that all participants exchanging data across borders are compliant with the organization's FIPs-based privacy framework, among other things.[30] In federated governments such as the United States, a common language of privacy helped states harmonize their laws around a common goal and minimize conflicts for industry.[31] In short, a common language of privacy provides interoperability, relative harmony, and incremental change. It helps avoid lurches that deviate too far from established understandings of privacy. Without the FIPs, countries and states

25. *See Data Transfers Outside the EU*, *supra* note 19.

26. *See generally* GREENLEAF, *supra* note 2; Gellman, *supra* note 11. A related version of the FIPs was incorporated into the Asia-Pacific Economic Cooperation ("APEC") Privacy Framework. *See* GREENLEAF, *supra* note 2, at 562–63.

27. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 and 42 U.S.C.).

28. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

29. *See Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV, http://2016.export.gov/safeharbor/eu/eg_main_018365.asp (last updated Jan. 12, 2017); *EU-U.S. Privacy Shield*, U.S. DEP'T OF COMMERCE, https://www.privacyshield.gov/welcome (last visited May 17, 2017).

30. *Cross Border Privacy Rules System*, ASIA-PAC. ECON COOPERATION http://www.cbprs.org/ (last visited May 17, 2017).

31. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 749 (2016) ("In the 1990s, while the Federal Trade Commission (FTC) was emphasizing self-regulation, state attorneys general were arguing that consumer protection laws required the adoption of Fair Information Practice Principles (FIPPs).").

would risk talking past each other every time they needed to cooperate on privacy issues.

B. Malleable and Severable

Another advantage of the FIPs is that they are malleable enough to serve as the building blocks for new regulatory proposals. In this way, progress is achieved incrementally rather than requiring an entire upheaval of privacy standards. One benefit to such general standards is that they can be clarified in response to specific problems. For example, Daniel Solove and Chris Hoofnagle have proposed a model data protection regime that adds more substance to the FIPs. The authors suggested that the United States is unlikely to shift from its sectoral approach to an omnibus one like Europe's, but even the sectoral approach can be improved by applying the FIPs.[32] David Hoffman, Associate General Counsel and Global Privacy Officer at Intel, has argued that "[t]he OECD FIPPs are foundational, and do not need to be changed. They do, however, need to be implemented in new ways to properly adjust to an environment of the internet of things, cloud computing, and advanced data analytics."[33] The relative ambiguity of the FIPs, though, also creates room for trouble. Fred Cate has been critical of the FIPs and has argued that lawmakers should "reclaim the original broader concept of FIPPs by adhering to Consumer Privacy Protection Principles (CPPPs) that include substantive restrictions on data processing designed to prevent specific harms."[34]

The FIPs are also severable, meaning that countries can adopt as many or as few of them as they wish. They are "mix and match" principles in practice, even if the drafters thought that all of them must be followed to be fully fair. In his history of the FIPs, Robert Gellman wrote, "[w]hile there is broad international agreement on the substance of FIPs, different statements of FIPs sometimes look different. Further, statutory implementations of FIPs may vary in different countries, contexts, and sectors."[35] Gellman documented the many different ways the FIPs have been implemented, which vary according to the types of records and who the record keepers are. In the United States, various laws have incorporated only some of the FIPs for specific classes of record-keepers or categories of records. Industry compliance with the FIPs is still "voluntary and sporadic."[36] Gellman

32. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 357.

33. David Hoffman, *The Essential Link Between Privacy and Security: Optimizing for Both*, LAWFARE (May 3, 2016, 9:48 AM), https://www.lawfareblog.com/essential-link-between-privacy-and-security-optimizing-both.

34. Cate, *supra* note 1, at 343.

35. Gellman, *supra* note 11, at 19.

36. *Id.* at 19–20.

argued that "[*n*]*otice and choice* is sometimes presented as an implementation of FIPs, but it clearly falls well short of FIPs standards."[37] Incomplete versions of the FIPs can also be found in rules and reports issued by the FTC, Department of Health and Human Services ("HHS"), and Department of Homeland Security ("DHS"), as well as multiple reports out of the White House.[38] The United States is probably the most prominent country to only partially work the FIPs into its privacy regime. Nearly every other country that has addressed privacy has given a full-throated adoption of the FIPs as the bedrock substantive data protections.[39]

Of course, this severability has drawbacks. Fred Cate argued "one problem of basing a data protection regime on FIPPS is determining which set of FIPPS to apply. The OECD Guidelines provide eight, the E.U. data protection directive eleven, and the FTC principles only five (or four)."[40] Cate argued that the differences are often quite substantive: "For example, only the OECD Guidelines and APEC Framework provide an explicit collection limitation principle . . . ."[41]

C. A Better Litmus Test for Responsible Data Processors

One of the most frustrating things about the concept of privacy is its squishiness. The concept is so vague that it is often difficult to determine when we have suffered a privacy harm. We use words like "creepy" and "disturbing" when confronted with privacy-invasive technologies that bug us in a way that we just can't put our finger on.[42] At our worst, we cannot create a reasonably objective anchor for new privacy threats, and we fall

37. *Id.* at 20.

38. *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY 45 (2011), https://www.nist.gov/sites/default/files/documents/2016/12/08/ nsticstrategy.pdf; EXEC. OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 49–52 (2012) [hereinafter CONSUMER DATA PRIVACY], https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf; NAT'L SCI. & TECH. COUNCIL, EXEC. OFFICE OF THE PRESIDENT, A POLICY FRAMEWORK FOR THE 21ST CENTURY GRID: ENABLING OUR SECURE ENERGY FUTURE 46 (2011), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf; Gellman, *supra* note 11, at 19–34 (discussing the inclusion of the FIPS by the FTC, HHS, and DHS).

39. GREENLEAF, *supra* note 2, at 57–58.

40. Cate, *supra* note 1, at 353.

41. *Id.*

42. *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 61 (2013); Evan Selinger, *Why Do We Love to Call New Technologies "Creepy"?*, SLATE (Aug. 22, 2012, 3:30 AM), http://www.slate.com/articles/technology/future_tense/2012/08/facial_recognition_software_targeted_advertising_we_love_to_call_new_technologies_creepy_.html.

back on a Justice Stewart-like mentality in which we "know it when [we] see it."[43]

This clumsiness over identifying privacy harms limits what will work on a global scale. Thankfully, the FIPs provide more granularity and nuance to create a better litmus test for regulators, industry, and data subjects to determine when a data processor's actions have gone afoul. For example, when app developers collect geolocation data from users' mobile phones without telling them, instead of relying on creepiness or searching for a harm that isn't there, regulators can point to the fact that notice was not given to the data subject and that there was a lack of consent. While the FIPs are still generalized standards with proportionality requirements that lack clear lines, they focus enough on particular problems to provide a more objective measure of privacy than mere intuition while remaining in harmony with broadly adopted values like autonomy and fairness.

Of course, like many debates typified by the tension between general standards and specific rules, there can be costs to granularity in the law, as I'll cover below. Too much specificity makes laws rigid and insensitive to context, meaning they can be a poor fit in many situations. Specificity can also facilitate a "checkbox" compliance mentality that elevates a shallow compliance with specific rules over substantive fulfillment of the law's purpose.[44]

In sum, we're basically stuck with some version of the FIPs, but for many good reasons. They provide a privacy touchstone for regulators, industry, and the public. Such a polestar is needed because people regularly disagree about privacy policy. For example, is mere exposure from a data breach a harm, or is it only a harm when information is misused? Can we have privacy in public? Should there be a right to be forgotten? There's good room for debate on these issues. But when common ground must be found, we regularly count on the FIPs. Need a privacy regulatory regime acceptable to industry? Base it off the FIPs because it facilitates data processing. Need an industry practice that will keep regulators and the public happy? Just follow some version of the FIPs, which has the distinct advantage of being more or less the "industry standard." In theory, everyone

---

43. *Movie Day at the Supreme Court or "I Know It When I See It": A History of the Definition of Obscenity*, FINDLAW, http://corporate.findlaw.com/litigation-disputes/movie-day-at-the-supreme-court-or-i-know-it-when-i-see-it-a.html (last visited May 17, 2017).

44. *See* Tene & Polonetsky, *supra* note 42, at 83. Tene and Polonetsky explain:

> Privacy regulation—comprised primarily of the fair information privacy principles (FIPPs)—is a means to an end. When viewed as a stand-alone edifice, privacy regulation becomes almost meaningless, a bureaucratic box-ticking exercise involving notices that few users read and "consent" without information, volition, or choice. In order to avoid creep, companies must engage their consumers in a meaningful conversation to reduce suspicion and align interests and expectations. They need to frame relationships by setting the tone for new products or novel uses of information.

Id. (footnote omitted).

wins something. The only problem is that these days the FIPs are not enough.

II. THE FIPS ARE INDEQUATE

Griping about the FIPs is not new. Since their inception, critics have taken issue with both the substance of the FIPs as well as how they have been implemented. When the FIPs first rose to prominence in 1980, James Rule and his colleagues criticized the FIPs for their failure to meaningfully limit surveillance systems. They categorized the FIPs as "efficiency" principles that endeavored to smooth the harsh edges of information systems to operate better for both data controllers and data subjects, instead of substantively limiting data collection against the interests of data controllers.[45]

Rule and his colleagues also criticized the efficiency mission of the FIPs because it opportunistically allowed those who were engaging in mass, corrosive data collection to get the benefit of the perception of "privacy protection" though formalistic compliance. They wrote that under the FIPs' criteria, "organisations can claim to protect the privacy of those with whom they deal, even as they demand more and more data from them, and accumulate ever more power over their lives."[46] Graham Greenleaf noted that this fundamental tension in the FIPs remains today, with questions still asked too infrequently, "to what extent do and should data privacy principles and laws go beyond attempting to ensure the 'efficiency' of personal information systems, and provide means to limit and control the expansion of surveillance systems?"[47]

The efficiency goal of the FIPs has also led to problems in the way that these regimes have been implemented. Above all, FIPs regimes are designed to effectuate "consent" to data practices and "control" over information. Consent and control quickly turn FIPs-based privacy rules into formalistic exercises designed to extract consent and use the gift of control to saddle the data subject with the risk of loss for data misuse. Fred Cate criticized FIPs-based regimes that are centered around control, writing, "the control-based system of data protection, with its reliance on narrow, procedural FIPPS, is not working. The available evidence suggests that privacy is not better protected. The flurry of notices may give individuals some illusion of enhanced privacy, but the reality is far different."[48] Cate argued,

---

45. GREENLEAF, *supra* note 2, at 60–61 (citing JAMES RULE ET AL., THE POLITICS OF PRIVACY 93 (1980)).

46. *Id.* (quoting RULE ET AL., *supra* note 45, at 93); *see also* Claudia Diaz et al., *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923, 924–25 (2013) ("The notion of the data controller as a *trusted party* is ill at ease with the anti-surveillance gist of constitutional privacy and PETs.").

47. GREENLEAF, *supra* note 2, at 61.

48. Cate, *supra* note 1, at 342.

> The result is the worst of all worlds: privacy protection is not enhanced, individuals and businesses pay the cost of bureaucratic laws, and we have become so enamored with notice and choice that we have failed to develop better alternatives. The situation only grows worse as more states and nations develop inconsistent data protection laws with which they attempt to regulate increasingly global information flows.[49]

Lisa Austin has also criticized the consent and control approach to privacy, writing, "consent-based privacy models are inadequate in the face of contemporary information practices and the emerging corporate–state nexus that has created such a striking surveillance infrastructure on the internet."[50] Mark MacCarthy has criticized consent regimes because they can make any information practice legitimate, even truly corrosive ones.[51] And, of course, substantive and practical problems with the FIPs are compounded by the fact that FIPs-based regimes are entrenched and difficult to change.

The FIPs are not completely entrenched, however. They have been improved slightly. The OECD, European Union, and United States made a push in the 1990s to modify the FIPs and usher in what has been referred to as a "second generation" of FIPs.[52] The most important addition in terms of substantive privacy protection was the "purpose limitation" practice, which limited what data controllers can do with the information it collects. However, the second generation of FIPs is still strongly rooted in its original framework. Omer Tene has criticized this second generation of FIPs as inadequate because, among other things, it fails to update the definition of personal data, it still clings to and even broadens the central role of consent, and it remains "rooted on a linear approach to processing whereby an active 'data controller' collects information from a passive individual, and then stores, uses, or transfers it until its ultimate deletion."[53]

I agree with both the dominant intrinsic and instantiated critiques of the FIPs. The FIPs seem to have facilitated more surveillance and a shift in

---

49. *Id.*

50. Austin, *supra* note 1, at 189. Austin notes:

> [There is a] structural problem relating to *what* consent regulates. This model of privacy law regulates personal information, which includes information about an "identifiable" person. The problem is that this is an all-or-nothing model where FIPs apply in relation to the collection, use, and disclosure of personal information but not other forms . . . .

Id. at 137–38 (footnote omitted) (citing Lisa M. Austin, *Reviewing PIPEPA: Control, Privacy, and the Limit of Fair Information Practices*, 44 CANADIAN BUS. L.J. 21 (2006); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Paul M. Schwartz & Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011)).

51. *See generally* MacCarthy, *supra* note 1.

52. *See* GREENLEAF, *supra* note 2, at 55–57; Tene, *supra* note 1, at 1228–29.

53. Tene, *supra* note 1, at 1219.

power to data collectors that a more robust resistance to the data complex might have prevented. And as you'll see below, I also lament the obsession of some FIPs regimes with formalistic compliance through consent instead of a more meaningful form of accountability.

However, in this Essay, I will focus on a few critiques of the FIPs that have not been given enough attention. The FIPs are inadequate because: (1) they have important blind spots regarding the collection, use, and disclosure of personal information that cannot be resolved through more specificity or better implementation; and (2) they fail to address the user bandwidth problem that would persist even if users were given every bit of control imaginable over their data.

The FIPs were first developed before most people even imagined owning a personal computer. They were designed to handle the issues that resulted from the collection and conversion of information into storable, searchable databases. The reality of everyone having a supercomputer, surveillance device, and beacon in their pockets with an accumulated digital universe of around 44 *trillion* gigabytes (!) was still a long way off.[54] Social media, biometrics, drones, and robots that interacted regularly with humans hadn't even been invented yet.[55] Yet here we are, with a new set of problems that the FIPs only partially address. We will need to get creative to solve them.

A. The FIPs Have Blind Spots

1. Our Vulnerabilities to Each Other

While the FIPs can be useful to articulate lofty design goals like transparency and data minimization, they are poor guides for setting design boundaries for information technologies for two main reasons: (1) they are primarily concerned with how data is controlled and processed and (2) they too often serve to elevate formalistic notions of "choice" and "control" over meaningful privacy protections.

The FIPs articulate desirable endpoints: openness, security, data quality, accountability, etc. However, they are mainly concerned with data collection, processing, and storage, not with the design that facilitates these actions. The FIPs do not directly address the effect of design signals and

54. *See* Bernard Marr, *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, FORBES (Sept. 30, 2015, 2:19 AM), http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#5b3c876f6c1d.

55. *See* M. Ryan Calo, *Robots and Privacy*, *in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 196 (Patrick Lin et al. eds., 2012); Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513 (2015); Hartzog, *supra* note 7; Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 IDAHO L. REV. 661 (2015); *see also* M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571 (2011); M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809 (2010).

transaction costs on trust, obscurity, and autonomy. The FIPs also fail to provide meaningful concrete guidance to lawmakers or companies regarding specific design choices like how to effectively disclaim or warn people regarding an important privacy-related practice or function.[56] Scholars like James Grimmelmann, Deirdre Mulligan, and Jennifer King have critiqued the FIPs as ineffective to guide the design of information technologies because they ignore the privacy problems inherent in the social exchange of information like social media.[57]

The FIPs are concerned with how powerful entities deal with aggregated personal information. But as James Grimmelmann noted, even if social media companies were completely compliant with the FIPs, "users would still create false profiles, snoop on each other, and struggle over the bounds of the private. For this reason, while reports dealing with privacy and other platforms often propose strong restrictions on data collection and transfer, the focus of reports on social-network-site privacy is appropriately elsewhere."[58] Lisa Austin has also noted these blind spots, arguing that "[w]e need to broaden our focus beyond consent and understand the importance of audience segregation, audience obligations, and practices of tact, and the role of social norms and roles."[59]

The basic framework of fair information practices was developed to address the issue of the collection, use and disclosure of personal information by large organizations, in the context of concerns regarding computer networks. The key relationship informing this privacy model is the individual-organization relationship. However, contemporary Internet companies increasingly operate as information intermediaries, mediating other types of relationships in complex ways. This raises a number of ques-

---

56. Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor wrote:

> Existing frameworks and processes for building privacy-friendly systems, such as Privacy by Design or privacy impact assessments, focus on the analysis of a system's data practices and less so on the design of notices. Even the OECD report on "making privacy notices simple" basically states that one should design a simplified notice, conduct usability tests, and deploy it—the crucial point of *how* to design a simplified notice is not addressed.

Florian Schaub et al., *A Design Space for Effective Privacy Notices*, 11 PROCEEDINGS OF THE SYMP. ON USABLE PRIVACY AND SECURITY 1–2 (2015) (footnotes omitted) (first citing G. DANEZIS ET AL., EUR. UNION AGENCY FOR NETWORK AND INFO. SEC., PRIVACY AND DATA PROTECTION BY DESIGN–FROM POLICY TO ENGINEERING (2014); then citing PRIVACY IMPACT ASSESSMENT FRAMEWORK CONSORTIUM, A PRIVACY IMPACT ASSESSMENT FRAMEWORK FOR DATA PROTECTION AND PRIVACY RIGHTS (David Wright et al. eds., 2011); and then citing OECD, MAKING PRIVACY NOTICES SIMPLE: AN OECD REPORT AND RECOMMENDATIONS 120 (2006), https://www.privacy.org.nz/assets/Files/International-APPA-APEC/Making-Privacy-Notices-Simple-An-OECD-Report-and-Recommendations.pdf). *See* OECD, *supra*, at 2–7.

57. *See* James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L.J. 793, 820 (2010); Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 993 (2012).

58. Grimmelmann, *supra* note 6, at 1189.

59. Austin, *supra* note 1, at 183.

tions regarding how a regime modeled on one type of relationship can regulate practices that in fact cover multiple, often intersecting, relationships.[60]

Consider social media. Unlike, say, your banking app, social media have two distinct audiences for your information: platforms and people. These two audiences present overlapping but distinguishable privacy issues. Platforms, meaning the companies that provide the social media software, are squarely the concern of the FIPs because they have robust concentrations of electronic information aggregated into colossal databases.[61] These platforms are risky because of how much data they can obtain from you and the fact that they control the terms of your mediated experience. After all, it is the company that designs the software.

Social relationships are risky to manage online because it is difficult to assess social risk at scale and the boundaries of social relationships have blurry edges.[62] In other words, while the harm from platforms is usually enabled by the aggregation of lots of data by one entity, the harm from people is often that one piece of information is exposed to the *wrong* audience. And these two distinct information recipients, platforms and people, present different challenges. Platforms are dangerous because of the power imbalance between platforms and users. People are dangerous because social interaction is messy and contextual with a vengeance.[63] And the FIPs have nothing to say about other people.

2. Our Susceptibility to Manipulation

One of our more endearing traits as humans is also one of our biggest weaknesses—we want to believe. The literature is full of examples of how people behave in predictably irrational ways. I have written elsewhere that "[h]umans rely too much on available anecdotes and judgments reached by computers. We attribute human emotions and agency to machines. We care too much what others think about us and we increasingly entrench ourselves in opinions formed based on trivial, anecdotal, and arbitrary evidence."[64] And these biases are regularly exploited by those with something to gain from it.

---

60. *Id.*

61. Bruce Schneier, *A Revised Taxonomy of Social Networking Data*, SCHNEIER ON SECURITY (Aug. 10, 2010, 6:51 AM), http://www.schneier.com/blog/archives/2010/08/a_taxonomy_of _s_1.html; *see also* Bruce Schneier, *A Taxonomy of Social Networking Data*, 8 IEEE SECURITY & PRIVACY 88, 88 (2010).

62. *See* Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1315 (2009); Grimmelmann, *supra* note 6.

63. For more information including principles regulating social data, see Woodrow Hartzog, *Social Data*, 74 OHIO ST. L.J. 995 (2013).

64. Hartzog, *supra* note 7, at 802 (first citing DANIEL KAHNEMAN, THINKING FAST AND SLOW (2013); DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS (2d ed. 2009); DANIEL THAYER & CASS SUNSTEIN, NUDGE: IMPROVISING DECISIONS

Here's the problem. Mediated experiences like interactions with user interfaces or even robots can be designed to exploit those vulnerabilities. Ryan Calo has observed that personal information is often leverage to mass produce bias, systemically ratchet-up disclosures, and target based on people's means.[65] He calls this a kind of "digital market manipulation." Kate Darling has argued that our tendency to emotionally invest in robots is worth paying attention to because of just how deep these connections run.[66] When a robot moves, talks, or looks alive, we tend to over-ascribe them with agency, intelligence, emotion, and feeling. Calo agrees, noting, "[t]here is an extensive literature to support the claim that people are 'hard-wired' to react to anthropomorphic technology such as robots as though a person were actually present. The tendency is so strong that soldiers have reportedly risked their own lives to 'save' a military robot in the field."[67]

In previous research, I have asked: "How might [human-like] robots affect the elderly, for whom robots have great potential as companions? Or what about children, who have difficulty parsing complex emotional attachments and understanding how robots work?"[68] Research has shown that children think of robots as friends and tell them secrets.[69] Kids' toys are ripe to be designed to simulate and stimulate emotional bonds and manipulate children to share information.

The FIPs have little to say about our susceptibility to manipulation. User interfaces can be designed to extract our "consent" or to encourage us to disclose in ways that we do not even notice. Visual rhetoric, anthropomorphism, and other psychological tools can be deployed in the shadow of the FIPs, which demand only transparency as to data collection and use practices. Data that is collected with our consent can be leveraged against us. The FIPs do not articulate any meaningful limits on companies who

---

ABOUT HEALTH, WEALTH, AND HAPPINESS (2d ed. 2009); then citing Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2007); and then citing Kate Darling, Extending Legal Rights to Social Robots (April 2012) (unpublished manuscript), http://robots.law.miami.edu/wp-content/uploads/2012/04/Darling_Extending-Legal-Rights-to-Social-Robots-v2.pdf).

65. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1006–07 (2014).

66. Darling, *supra* note 64.

67. RYAN CALO, BROOKINGS, THE CASE FOR A FEDERAL ROBOTICS COMMISSION (2014), http://www.brookings.edu/research/reports2/2014/09/case-for-federal-robotics-commission (citing P.W. SINGER, WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE TWENTY-FIRST CENTURY 337–43 (2009)).

68. Hartzog, *supra* note 7, at 806 (citing *A Robotic Companion for the Elderly?*, GE IDEA LAB (Aug. 13, 2014), http://www.ideaslaboratory.com/post/94619189589/a-robotic-companion-for-the-elderly). *But see* Amanda Sharkey & Noel Sharkey, *Granny and the Robots: Ethical Issues in Robot Care for the Elderly*, 14 ETHICS AND INFO. TECH. 27 (2012).

69. Jacqueline Kory Westlund & Cynthia Breazeal, *Deception, Secrets, Children, and Robots: What's Acceptable?*, 10 ACM/IEE INTERNATIONAL CONFERENCE ON HUMAN-ROBOT INTERACTION 1–2 (2015), http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Mf-Westlund.pdf.

would use our own cognitive limitations against us or give any clear sense of when companies have crossed an ethical line in using our own data in trying to persuade us to share more, click an ad, or make a purchase online. Given the increasing efficacy of machine learning and big data, this threat will only continue to grow.

3. Our Helplessness to Automated Decisionmaking

Big Data and algorithms promise to revolutionize the decisionmaking process of organizations. Decisions that used to be made by humans based upon a small amount of information are now going to be made by automated software based upon exabytes of data.[70] Danielle Citron noted that where humans used to rely upon computers merely to help them make decisions, automated systems have increasingly become the primary decisionmakers.[71] She explained that these systems take humans out of the loop when terminating individuals' Medicaid, food stamp, other welfare benefits, and the process of targeting people for exclusion from air travel.[72] Moreover, she observed that "[c]omputer programs identify parents believed to owe child support and instruct state agencies to file collection proceedings against those individuals. Voters are purged from the rolls without notice, and small businesses are deemed ineligible for federal contracts."[73] This raises some serious issues, including threats to due process,[74] disparate impact on minority and other vulnerable communities,[75] invasions of privacy and stigmatization due to the powerful predictive power of data analytics,[76] and more.

What's worse, opting out of automated decisionmaking soon won't even be an option. If governments embrace scoring systems similar to credit scores—but for everything—we risk turning into what Frank Pasquale and Danielle Citron call a "scored society."[77] Even without government as-

---

70. An exabyte is 1 billion gigabytes. Daniel Price, *Surprising Facts and Stats About the Big Data Industry*, CLOUDTWEAKS (Mar. 17, 2015), http://cloudtweaks.com/2015/03/surprising-facts-and-stats-about-the-big-data-industry/.

71. Citron, *supra* note 64, at 1252.

72. *Id.*

73. *Id.* (footnotes omitted) (first citing Susannah Zak Figura, *Where's Dad?*, GOV'T. EXEC., Dec. 1, 1998, at 12; then citing Letter from Juliet T. Hodgkins, Gen. Counsel, U.S. Election Assistance Comm'n, to Sarah Ball Johnson, Executive Dir., Ky. State Bd. of Elections (May 11, 2006) (on file with Danielle Keats Citron); then citing Denise Kersten, *Bytes vs. Brains*, GOV'T EXEC., Sept. 1, 2005, at 30).

74. *See id.* at 1249.

75. *See* Barocas & Selbst, *supra* note 6.

76. Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 83 (2013).

77. Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 8 (2014); *see also* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 191 (2015); Tal

sistance, the general zeal in industry to score everything so that it may be ranked, filed, and sorted will increasingly subjugate the public to the sorting whims of companies deploying algorithms.[78] We're seeing the seeds of this right now. China is moving to "give every citizen a score based on behavior such as spending habits, turnstile violations and filial piety, which can blacklist citizens from loans, jobs, [and] air travel."[79] Autonomous systems can be a force for good, but their value is not inherent. Whether they are beneficial is entirely dependent upon who is using them and how they are deployed.

Kate Crawford and Ryan Calo have argued, "[a]utonomous systems are already deployed in our most crucial social institutions, from hospitals to courtrooms. Yet there are no agreed methods to assess the sustained effects of such applications on human populations."[80] The authors argue that there is a need to assess the impact of automated technologies in their social, cultural and political settings.

For example, Crawford and Calo wrote that research is needed to determine "how the app AiCure—which tracks patients' adherence to taking prescribed medication and transmits records to physicians—is changing the doctor–patient relationship."[81] Or perhaps researchers would "explore whether the use of historical data to predict where crimes will happen is driving overpolicing of marginalized communities."[82] Or maybe researchers might ask, "why high-rolling investors are given the right to understand the financial decisions made on their behalf by humans and algorithms, whereas low-income loan seekers are often left to wonder why their requests have been rejected."[83]

The FIPs alone will not provide a framework for answering or responding to these questions. They might be able to affect the periphery of autonomous decisionmaking problems by limiting the corpus of data used in decisionmaking systems. But the FIPs do not address the major, structural problems inherent in automated systems, including the fact that it is very difficult to erase bias from autonomous systems because of the biased humans creating them, the fact that the cost of these systems are not borne equally by all members of society, and the fact that people tend to irration-

---

Z. Zarsky, *Understanding Discrimination in the Scored Society*, 89 WASH. L. REV. 1375, 1375 (2014); Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1740, 1745 (2015).

78. *See* PASQUALE, *supra* note 77, at 69.

79. Josh Chin & Gillian Wong, *China's New Tool for Social Control: A Credit Rating for Everything*, WALL ST. J. (Nov. 28, 2016, 11:46 AM), http://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590.

80. Kate Crawford & Ryan Calo, *There Is a Blind Spot in AI Research*, NATURE (Oct. 13, 2016), http://www.nature.com/news/there-is-a-blind-spot-in-ai-research-1.20805.

81. *Id.*

82. *Id.*

83. *Id.*

ally trust conclusions reached by computers more than conclusions reached by humans, solely because of their automated nature—a phenomenon known as "automation bias."[84] While the FIPs protect the integrity and fairness of databases themselves, they do not fully address the risks inherent in automated decisionmaking systems.

B. The FIPs Have a Bandwidth Problem

Let me be blunt: privacy regulators and designers have made a big mistake by hinging virtually everything on FIPs-based regimes centered around the idea of control or consent. Control has become a talisman for privacy protection.[85] This is a problem because control is a critical finite resource for people. Yet FIPs-based data protection regimes treat it like a bottomless well.

In theory, the goal of the FIPs is to empower data subjects. To empower in this context means to put in control—to ensure that data subjects (1) have knowledge of a data collector's activities and (2) give consent for certain practices. Knowing companies' data practices and requiring them to seek your consent for any material thing they want to do sounds good in theory. It ostensibly helps people decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information.

Control has become the archetype for data protection regimes. It is the first right articulated in the Obama Administration's proposed "Consumer Privacy Bill of Rights."[86] Control was also a major component of the FTC's report on "Protecting Consumer Privacy in an Era of Rapid

84. *See* Citron, *supra* note 65, at 1271–72. As Citron explained it:

> Studies show that human beings rely on automated decisions even when they suspect system malfunction. The impulse to follow a computer's recommendation flows from human "automation bias"—the "use of automation as a heuristic replacement for vigilant information seeking and processing." Automation bias effectively turns a computer program's suggested answer into a trusted final decision.

Id. (footnotes omitted) (first citing Raja Parasuraman & Christopher A. Miller, *Trust and Etiquette in High-Criticality Automated Systems*, 47 COMM. ACM 51, 52 (2004); then quoting Linda J. Skitka et al., *Automation Bias and Errors: Are Crews Better Than Individuals?*, 10 INT'L J. AVIATION PSYCHOL. 85, 86 (2000); and then citing M.L. Cummings, *The Social and Ethical Impact of Decision Support Interface Design*, *in* INTERNATIONAL ENCYCLOPEDIA OF ERGONOMICS AND HUMAN FACTORS 1, 7 (Waldemar Karwowski ed., 2d. ed. 2006)).

85. For additional critiques of the "consent" model for effectuating the FIPs, see, for example, Kevin D. Haggerty, *What's Wrong With Privacy Protections? Provocations from a Fifth Columnist*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 190, 190–91 (Austin Sarat ed. 2015), Lisa M. Austin, *Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA*, 56 U. TORONTO L.J. 181 (2006), Cate, *supra* note 1, and Tene & Polonetsky, *supra* note 5.

86. CONSUMER DATA PRIVACY, *supra* note 38, at 1.

Change."[87] Consent is the linchpin of the entire European Union's GDPR. It legitimizes most kinds of data collection, use, and disclosure.[88]

In fact, control over information is often floated as the very definition of privacy itself. The great privacy scholar Alan Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[89] Others, including Arthur Miller, Charles Fried, Ferdinand Schoeman, and Richard Parker, conceptualize privacy in terms of control as well.[90] Countless popular press articles and books are aimed at helping us "take control" of our privacy online.[91] Indeed, technology companies seem to be making a good faith effort to gradually increase and simplify user control where appropriate.[92]

Control is an industry favorite privacy tool as well. To hear tech companies tell it, the answer to modern privacy problems is just to give users more control. Employees from Facebook have stated, their "philosophy that people own their information and control who they share it with has remained constant."[93] Facebook founder and CEO Mark Zuckerberg said, "[w]hat people want isn't complete privacy. It isn't that they want secrecy. It's that they want control over what they share and what they don't."[94] Microsoft CEO Satya Nadella summarized his company's focus on user control stating, "Microsoft experiences will be unique as they will . . . keep a user in control of their privacy[,]" adding that the company will

87. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

88. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 7 ("In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis . . . .").

89. ALAN WESTIN, PRIVACY AND FREEDOM 5 (2015) (1967).

90. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 24–25 (2008).

91. *See, e.g.*, JOE KISSELL, TAKE CONTROL OF YOUR ONLINE PRIVACY (2015); *Privacy Survival Guide: Take Control of Your Personal Information*, PRIVACY RIGHTS CLEARINGHOUSE, 1997 (Bulletin); *5 Ways to Control your Privacy on Google*, USA TODAY (Mar. 16, 2012, 3:30 PM), http://usatoday30.usatoday.com/tech/news/story/2012-03-17/google-privacy-settings/53573266/1; Eric Griffith, *Take Control of Your Google Privacy*, PC MAG. (June 25, 2015), http://www.pcmag.com/article2/0,2817,2486726,00.asp.

92. *See, e.g.*, Jules Polonetsky, *Facebook's Privacy Dinosaur*, LINKEDIN (Mar. 26, 2014), https://www.linkedin.com/pulse/20140326110913-258347-facebook-s-privacy-dinosaur.

93. Kathy H. Chan, *On Facebook, People Own and Control Their Information*, FACEBOOK (Feb. 16, 2009, 5:09 PM), https://www.facebook.com/notes/facebook/on-facebook-people-own-and-control-their-information/54434097130.

94. Michael Zimmer, *Mark Zuckerberg's Theory of Privacy*, WASH. POST (Feb. 3, 2014), https://www.washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html (quoting a 2010 interview by *Time Magazine* with Mark Zuckerberg).

"[a]dvocat[e] laws and legal processes that keep people in control."[95] Google has written, "Google builds simple, powerful privacy and security tools that keep your information safe and put you in control of it."[96] There is seemingly no privacy problem for governments or technology companies that more user control cannot fix. Just chuck some more control at it.

In theory, this is a laudable goal. In practice, it hasn't worked out so well. There are two problems with elevating control. First, control doesn't scale. The sheer number of choices that inundate users under a control regime is overwhelming to the point of futility. Second, the other FIPs become subservient. Fixation on control sidelines other important principles, such as limiting data collection in the first place.

Professor Neil Richards and I have cautioned against over-relying on the notion of control to protect privacy.[97] We call this misguided allegiance to control the "Control Illusion." The Control Illusion dominates privacy policy as well as public discourse. When the FTC first started to regulate privacy in the late 1990s, it adopted a basic control scheme for businesses dubbed "notice and choice." People were said to have "control" over their information when they were notified about a company's information collection, use, and disclosure practices and given a choice to opt out (usually by not using the service). Failure to opt-out acts as a permission slip for companies, so long as they act within the boundaries of that ubiquitous, readable block of text called the privacy policy.[98] Through notice and choice, "control" is leveraged to become a little more than a mechanism optimized to generate consent.

The problem with notice, choice, and control is that it is impossible to scale. No one can read all the privacy policies they come across.[99] People have lives to get on with and if they took the time to read and make sure they understand all the terms of use they came across, they would do little

95. *Data Privacy Day 2015—Putting People in Control*, MICROSOFT CORP. BLOGS (Jan. 28, 2015), http://blogs.microsoft.com/on-the-issues/2015/01/28/data-privacy-day-2015-putting-people-control/ (quoting an e-mail from Satya Nadella, CEO Microsoft, to Microsoft employees).

96. Guemmy Kim, *Keeping Your Personal Information Private and Safe—And Putting You in Control*, OFFICIAL GOOGLE BLOG (June 1, 2015), https://googleblog.blogspot.com/2015/06/privacy-security-tools-improvements.html.

97. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016).

98. *Id.* at 444–47.

99. Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/; *see also* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543 (2008).

else. What's worse is that we cannot escape the boilerplate. Living offline simply isn't an option in the modern world.[100]

The "control" we get ends up being too much of a good thing. From the moment people boot up a device, they are gifted with "control" over information in the form of privacy policies, terms of use, and pop-up banners for each and every website or app you visit or use. The incessant onslaught is enough to make anyone's eyes gloss over and click on whatever is presented to us, just so we can finally use the service. Some regulators are coming around to the futility of notice and the absence of real choice about the pervasive collection of personal data. The White House Privacy and Civil Liberties Oversight Board recognized as much in its long-awaited report on privacy and surveillance.[101] In its report on Big Data, the White House also questioned the ongoing validity of the "notice and consent" approach to data protection.[102]

Even the FTC has realized the limits of notice and choice.[103] The agency's report on protecting consumer privacy in the digital age acknowledged that "the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity."[104] Yet despite the acknowledgment that notice and choice cannot do the work we ask of it, the mantra of user control persists.

---

100. JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 41 (2014).

101. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 137 (2014).

102. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 54 (2014); *see also* FED. COMMUNICATIONS COMM'N., FACT SHEET: THE FCC ADOPTS ORDER TO GIVE BROADBAND CONSUMERS INCREASED CHOICE OVER THEIR PERSONAL INFORMATION, https://apps.fcc.gov/edocs_public/attachmatch/DOC-341938A1.pdf (last visited May 17, 2017) (demonstrating that the FCC's proposed broadband privacy rules also inherently recognize the limitations of the old notice and consent model by providing rules that focus on meaningful consent and opt-ins as opposed to opt-outs).

103. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the Annual Conference on Privacy & Data Security Law: Proskauer on Privacy (Oct. 19, 2010) ("[T]he Notice and Choice model, as it is often deployed today, places too great a burden on consumers."); Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009) ("We do feel that the approaches we've tried so far—both the notice and choice regime, and later the harm-based approach—haven't worked quite as well as we would like.").

104. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 20 (2010). The report also acknowledged the limits of privacy harm stating:

> The FTC's harm-based approach also has limitations. In general, it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives. But, for some consumers, the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information "out there."

Id.

There is hope for control as an aspect of privacy. We simply must stop treating it as though it were an infinite resource. It's a little like the problem of trying to remember all of your passwords. You may be able to remember a few, but it is almost impossible to remember them all. Control is too precious for companies and lawmakers to over-leverage it. Control can enable autonomy, but it is not the same thing as autonomy. Any sound approach to privacy must ensure the right amount of control, autonomy, and freedom of choice for people. The problem comes when the pursuit of control becomes the *main* or *only* way companies address privacy.

At best, prioritizing "control" of our personal information over other goals, like enforcing trust obligations and minimizing data collection, is fool's gold. At worst, it's a trap. Psychologist Barry Schwartz argued in *The Paradox of Choice* that while autonomy and freedom of choice are critical human values, too many choices and too much control can actually overwhelm and confuse us.[105] Professors Idris Adjerid, Alessandro Acquisti, and George Loewenstein called upon this notion to argue that choice mechanisms without supplemental protections are likely to mislead consumers, quelling their privacy concerns without providing meaningful protection.[106] People feel falsely empowered by opportunities to restrict the collection and use of their personal information.

Control regimes can also shift the burden of responsibility for protecting privacy to people who are less equipped to handle it. The modern data ecosystem is hopelessly complex and opaque. Data subjects have the fewest resources of every party in the chain of data flows and they are on the wrong side of substantial information and power disparities. While control is an attractive goal in isolation, it comes with a practical and legal *obligation*. If you do not exercise that control, you are at risk. Companies can take your inaction as acquiescence.

In the aggregate, the weight of too much control will crush us. It will leave us bewildered, hopeless, and agreeable to anything. Privacy policies become "anti-privacy policies" because companies know that we will never read them. The default settings for privacy controls are permissive, because companies know that we do not usually change them. Retail stores tracking your devices only let you opt out online instead of in the store because they know you probably will not remember or make the effort to do so later.[107] Control is a vital but scarce resource. It is easily diluted. Adversarial design can make the downsides to control worse. Prioritizing control hides

105. BARRY SCHWARTZ, THE PARADOX OF CHOICE: WHY MORE IS LESS (2005).

106. Idris Adjerid et al., Framing and the Malleability of Privacy Choices (unpublished manuscript) http://www.econinfosec.org/archive/weis2014/papers/AdjeridAcquistiLoewenstein-WEIS2014.pdf (last visited May 17, 2017).

107. Press Release, Fed. Trade Comm'n, Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices (Apr. 23, 2015), https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers.

the power imbalances inherent in our modern mediated lives. Privacy regimes should seek to preserve control for when it can be the most effective, and leave the rest to other concepts, like privacy-friendly design.

III. A SHIFT TO DESIGN: THE FIPS AS A GOOD START

If the FIPs are not enough, then what is needed? What are the best alternatives to control in light of the fact that regulators are unlikely to abandon the FIPs? In a sense, modern privacy law is still all about "control," but its locus has shifted from individuals' control over their own information to the control that others can exert over someone by virtue of the information they possess.[108] In other words, modern privacy law is not about choice. It's about abuse of power.[109] In that light, the most obvious areas of law to bring into privacy law's fold are those principally concerned with abuse of power, such as antitrust, unfair competition law and anti-discrimination law.

A. The Future of Privacy is in the Market, the Mind, and the Machine

Big data has made the market more important to privacy law than ever before. Maurice Stucke and Allan Grunes argued that modern data practices raise both privacy and antitrust concerns.[110] The authors observe that mergers can "lessen non-price competition in terms of the array of privacy protections offered to consumers. Likewise, monopolies' data-driven exclusionary practices can hamper innovative alternatives that afford consumers greater privacy protection."[111] Many companies do not face pressure to truly compete on privacy. The authors argue that market forces are not currently solving privacy issues and that data-driven industries are subject to network effects, increasing the power of Big Data to exploit data subjects.[112] Chris Hoofnagle has advocated for an evolved role for the FTC's Bureau of Economics (BE) in identifying and encouraging a more robust market for privacy.[113] Peter Swire has argued that the FTC should consider

108. *See, e.g.*, Calo, *supra* note 65.

109. *See* Austin, *supra* note 1, at 159.

110. STUCKE & GRUNES, *supra* note 10; *see also* Chris Jay Hoofnagle, *The Federal Trade Commission's Inner Privacy Struggle* 1, 15, 18 (U.C. Berkeley Public Law Research, Paper No. 2901526, 2017).

111. STUCKE & GRUNES, *supra* note 10, at 4.

112. *Id.*

113. *See* Hoofnagle, *supra* note 110, at 18 ("Elucidating areas where some valuation of privacy exists—particularly in business to business scenarios where actors actually read policies and have the resources and time to protect rights—could help establish a value for privacy.").

privacy impacts in assessing mergers.[114] From here on out, privacy law must take market power more seriously.

Privacy law must also deal with the machines. We're going to need a whole new approach to artificial intelligence ("AI") if it is to be a sustainable technology. To begin, the FIP of data minimization principle is at odds with refining AI systems and mitigating the bias inherent in the systems. AI needs a steady stream of good, quality data to improve. One way to approach this is to shift away from a FIPs mindset to one that focuses on other problems besides just data collection. Crawford and Calo have argued in favor of a "social-systems" analysis of automated systems that run on data. They wrote:

> A practical and broadly applicable social-systems analysis thinks through all the possible effects of AI systems on all parties. It also engages with social impacts at every stage—conception, design, deployment and regulation.
>
> As a first step, researchers—across a range of disciplines, government departments and industry—need to start investigating how differences in communities' access to information, wealth and basic services shape the data that AI systems train on.[115]

This attention to the secondary effects of the data used in AI systems will be an important new turn for privacy law. The "garbage in, garbage

---

114. Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS (Oct. 19, 2007, 9:00 AM), https://www.americanprogress.org/issues/economy/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/. Swire argues:

> [I]t is logical to consider privacy remedies as part of merger analysis. Traditional antitrust analysis examines a proposed merger and often sets conditions on approval—the merger can proceed for aspects that create consumer welfare, but cannot proceed for aspects where harms outweigh the benefits. Where consumers suffer from lower product quality and reduction of consumer welfare, such as through privacy harms, it thus is logically consistent to consider merger conditions that address privacy harms.

Id.; *see also* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335 (2013).

115. Crawford & Calo, *supra* note 80. Crawford and Calo continue:

> A social-systems analysis could similarly ask whether and when people affected by AI systems get to ask questions about how such systems work. Financial advisers have been historically limited in the ways they can deploy machine learning because clients expect them to unpack and explain all decisions. Yet so far, individuals who are already subjected to determinations resulting from AI have no analogous power.
>
> A social-systems analysis needs to draw on philosophy, law, sociology, anthropology and science-and-technology studies, among other disciplines. It must also turn to studies of how social, political and cultural values affect and are affected by technological change and scientific research. Only by asking broader questions about the impacts of AI can we generate a more holistic and integrated understanding than that obtained by analysing aspects of AI in silos such as computer science or criminology.

Id. (footnote omitted) (citing KATE CRAWFORD ET AL., THE AI NOW REPORT: THE SOCIAL AND ECONOMIC IMPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE NEAR-TERM (2016)).

out" problem of big data and automated systems can instantiate wrongful discrimination and have a disparate impact on minority and vulnerable populations.[116] It can subject people to a confusing, opaque system of automated decisionmaking and credit scoring that denies them due process. These are the kinds of harms aimed to be remedied by anti-discrimination laws and civil rights. While privacy law has always had a close relationship to the law designed to prevent abuses of power, it is time to make that connection much more explicit.

Finally, privacy law must deal with the mind. Specifically, privacy law should focus just as much on people's expectations and mental models when they share their information as it does on how entities process data. This means focusing on the thing that shapes user expectations and use that has thus far been largely missing from FIPs-based privacy regimes around the world—the design of technologies. In the next Section, I'll advocate a turn to design for privacy law.

B. Privacy Law Should Focus on Design

One of the largest problems with the FIPs is that they do not directly address the design of technologies. By design, I mean the entire universe of people and processes that create technologies and the results of their creative process instantiated in hardware and software. FIPs-based regimes typically speak to the processing of data, but are relatively silent about what the instrumentalities of data collection, use, and disclosure should look like, or how they are built, or how they should function. For example, traditional inquiries into whether the kind of notice given to users have traditionally focused on the words that were used in privacy policies and terms of use. Design elements like fonts, graphic design, symbols, structures, or other contextual factors that might affect a user's expectations are often overlooked. While words are an easy way to measure transparency, they do not tell the whole story of what shapes people's risk assessments and understanding of terms when using technologies. The FIPs are more concerned with data processing obligations than user expectations.

This is a problem because there are overwhelming incentives to design technologies in a way that maximizes the collection, use, and disclosure of personal information. Companies can profit by designing their technologies to marginalize users' interests in transparency and ability to meaningfully control (or limit) over how their data is collected and used. When regimes that are built upon the FIPs are silent about how the technologies that peo-

116. *See* CLAIRE GARVIE ET AL., GEO. L. CTR. PRIVACY & TECH., THE PERPETUAL LINEUP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA (2016); Barocas & Selbst, *supra* note 6; Citron & Pasquale, *supra* note 77; Zarsky, *supra* note 77, at 1412; Andrew P. Selbst, Disparate Impact in Big Data Policing (Jan. 18, 2017) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2819182.

ple use are built, design can be leveraged in subtle ways to get more, more, more. For example, symbols and icons like padlocks and seals can be used to make users feel like it is safe to disclose personal information online.[117] Ambiguous "privacy settings" and other semantically vague buttons like "add friends" can give users the wrong impression about the risks and reality of personal disclosure.[118]

Privacy law should more explicitly address the design of consumer technologies. A logical approach to design can answer pressing questions in the privacy debate. How far can governments go in crippling privacy-protective technologies like encryption? Should surveillance technologies be designed to be undetectable? What technical safeguards should companies be required to use to protect their users' data? What should be the limits of nudging, default settings, and structured choice on social media? In short, the design of technologies is probably the largest gap in privacy law. By addressing design, privacy regimes can go beyond the FIPs while also ensuring they will continue to be meaningfully implemented.[119]

While design is no cure-all, it can be more effective than laws, terms of service, or organizational policies that restrict activity because design affects every user. People generally don't read the terms of use and they may not be aware of privacy laws, but every single person that uses an app must reckon with the constraints of technology.

Scholars have argued for years that design is (or at least should be) an important part of privacy regimes because of its power to affect human behavior at scale. Twenty years ago, Professor Joel Reidenberg argued that fair data protection rules could be enforced through technical design mechanisms that co-exist with privacy policy. He observed, "Technological capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations. Even user

117. *See* Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635 (2011).

118. *Id.* at 1631–36; Press Release, Fed. Trade Comm'n, Path Social Networking App Settles FTC Charges It Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.

119. The concept of "privacy by design" is already being robustly developed by scholars, regulators, and industry. One such approach was pioneered by former Information and Privacy Commissioner of Ontario, Ann Cavoukian. *See* Anne Cavoukian, Privacy By Design: The 7 Foundational Principles, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (last visited May 17, 2017); *see also* COURTNEY BOWMAN ET AL., THE ARCHITECTURE OF PRIVACY: ON ENGINEERING TECHNOLOGIES THAT CAN DELIVER TRUSTWORTHY SAFEGUARDS (2015); MICHELLE FINNERAN DENNEDY ET AL., THE PRIVACY ENGINEER'S MANIFESTO: GETTING FROM POLICY TO CODE TO QA TO VALUE (2014); E.U. INFO. COMMISSIONER'S OFFICE, THE GUIDE TO DATA PROTECTION (2017), https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/. *But see* Lee A. Bygrave, *Hardwiring Privacy*, *in* THE OXFORD HANDBOOK OF THE LAW AND REGULATION OF TECHNOLOGY (Roger Brownsword et al. eds., forthcoming).

preferences and technical choices create overarching, local default rules."[120] Reidenberg proposed, "in essence, that the set of rules for information flows imposed by technology and communication networks form a 'Lex Informatica' that policymakers must understand, consciously recognize, and encourage."[121]

Professor Lawrence Lessig popularized this notion that "code is law" in the late 1990s. Lessig argued that architecture like software code is a regulatory force on people similar to laws, norms, and the market.[122] Lessig wrote, "code presents the greatest threat to liberal or libertarian ideals, as well as their greatest promise. We can build, or architect, or code cyberspace to protect values we believe are fundamental, or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of *building*."[123] In his chapter on privacy in his influential book *Code and Other Laws of Cyberspace*, Lessig argued in favor of technologies as a way to provide choices about how our information is used and shared, limit information collection, and secure our data—all notions captured by the FIPs.[124]

Good design is proactive. If it works, then it protects against privacy harms before they even happen. Compare this to privacy law's current focus on conduct and harm. By definition, people have to wait until they have actually suffered before they can seek redress. If given the choice, we should seek to keep harms from happening at all. Even when relief is available to victims, it cannot make them "whole." The law strives to get as close as it can through money damages and injunctions, but most people who suffer harm would likely prefer to avoid the injury in the first place.

Adding a proactive protection like design to privacy law will help fill gaps in current privacy regimes. Design-based protections can require companies to protect against reasonably anticipated third-party harms.

---

120. Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554–55 (1998) [hereinafter Reidenberg, *Lex Informatica*] (footnotes omitted) (first citing Larry Lessig, *Reading in the Constitution in Cyberspace*, 45 EMORY L.J. 869, 896–97 (1996); then citing M. Ethan Katash, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 U. CHI. LEGAL F. 335; and then citing Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 918, 927–28 (1996)); *see also* Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 301–04 (1993) (arguing that technical considerations establish normative standards which, in turn, impact system practice); Reidenberg, *supra* note 1, at 508–09 (arguing that legal rules may be supplemented by technical considerations as well as business practices).

121. Reidenberg, *Lex Informatica*, *supra* note 120, at 555.

122. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 3 (1999) [hereinafter LESSIG, CODE AND OTHER LAWS]; Lessig, *supra* note 120, at 896–97; Lawrence Lessig, *Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 501–46 (1999).

123. LESSIG, CODE AND OTHER LAWS, *supra* note 122, at 6.

124. *See id.* at 200–32.

Technology users will not have to worry as much about hiring an attorney or suffering only to receive a paltry recovery because they will not become victims. Design cannot do everything, but it can dissuade would-be wrongdoers if the transaction cost is high enough.

IV. CONCLUSION

Some of the most pressing privacy problems over the next few decades might have sounded like the stuff of science fiction to those who first developed the fair information practices in the 1970s. Machines are going to get smarter. They will continue to make more critical decisions that used to be made by humans. The costs of these decisions will not be borne equally in society. People will become vulnerable to manipulation due to their attachment to robots that look and act like people and animals. Our own faces, eyes, and even ears will give away our identities, locations, and secrets. And, increasingly, more human interaction will be mediated by smartphone apps, virtual reality, and augmented reality. The architecture of those environments will dictate privacy outcomes every bit as much as what data controllers do with their databases because design picks data winners and data losers. All of these problems will amount to more than the established principals that demand transparency and accountability in database management can handle. Control over personal data alone is a poor fit to save us from ourselves, from each other, and from the machines.

But it would be misguided to try and marginalize the FIPs. In addition to being practically difficult to do, the benefits of the FIPs are far too valuable. The global digital economy demands some harmony among privacy regimes. Industry and society need to be able to find common ground on the boundaries of data collection and use. The FIPs reflect a shared wisdom about best data practices and have been remarkably resilient.

What is needed is a little more imagination and a willingness to admit that the FIPs are not the cosmos. The answer to every privacy problem cannot simply be "FIP harder." There is room on the world stage of privacy regulation to consider the rules relating to competition, anti-discrimination, and the design of information technologies. Recognizing the FIPs as a vital part, but not the whole, of privacy regimes is the only path to a sustainable future for privacy. The FIPs are dead. Long live the FIPs.