Michael Moretti
Docket No. 180821780—8780—01

Comments to the NTIA's Proposal on Consumer Privacy Protection

Introduction

The problems that persist in the existing notice and choice regime are not sufficiently resolved by the privacy outcomes as they are outlined in this proposal. Not only are the outcomes themselves lacking, but the proposal provides scant recommendation for how organizations can best effectuate the proffered privacy outcomes, or perhaps more troubling, how the law can be used to enforce privacy outcomes when organizations fail to do so—justifying this lack of guidance as an effort to avoid over-prescription. Nevertheless, there are ways of protecting consumer privacy without burdening innovation. More so, rather than assume policymaking must balance privacy interests against the costs to innovation, privacy law scholarship seems to suggest that both consumers and organizations can mutually benefit from privacy laws that promote trust in information relationships. However, this mutually beneficial arrangement cannot be achieved without first changing the way we think about privacy.

Therefore, the following commentary proceeds in two steps. The first part highlights what is missing from the privacy principles and contends that such insufficiency is the result of thinking about privacy in narrow and outdated ways. The second part provides a reinterpretation of the principles in light of thinking about privacy in terms of trust and then provides some examples of how the law can operationalize these reinterpreted, trust-promoting privacy principles.

Discussion

A. What is Missing from the Proposal's "Privacy Outcomes?"

Privacy Harm as a Harm

The proposal claims to have formulated its description of its privacy outcomes with an end-goal or focus on mitigating and managing "privacy harm" or the risk thereof. The proposal makes continued reference of this term "privacy harm" in each of its "privacy outcome" descriptions without actually explaining what it means. It seems incumbent on a policy proposal designed to develop consumer privacy protection to state what consumers need to be protected from. The lack of definition is problematic in itself since successful litigation of privacy claims has historically run up against the difficulty or barrier of concretizing injury.

Part of the reason for the difficulty of finding harm in a privacy claim is the notion that a plaintiff's previous disclosures constitute consent rendering the disclosed information no longer protectable. Furthermore, a plaintiff is oftentimes deemed to have assumed the risk because of such "consent." In addition, plaintiffs are also denied redress if it is found that they did not have a reasonable expectation of privacy. As a result, unprotected privacy interests manifest in a wide range of occasions, from photographed images of a couple kissing in public to revenge porn to the unauthorized sharing of information posted on social medial. These problems of defining privacy harm appear in tort law, statutory law, and even regulatory law.

Torts

In the realm of tort law, the four main privacy torts include appropriation of name or likeness, intrusion upon seclusion, false light, and the public disclosure of private facts. While these torts may have proved helpful in a pre-digital era, the privacy torts are ill suited to respond to problems arising from data collection and data use.[1] For instance, the tort of intrusion upon seclusion turns on the offensiveness of the manner in which information is gathered. However, this tort is not generally useful when it comes to accounting for data collection, since we are often willing to turn over our information. With respect to the appropriation tort, because oftentimes a finding of appropriation of name or likeness turns on whether the use of the name or likeness was done for

[1] *The FTC and the New Common Law of Privacy*, 114 Colum L. Rev. 583, 590 (2014)

commercial benefit, like advertising, courts have denied damages to plaintiffs because they have either failed to hold whether or not plaintiffs have any actual value in their personal information or they have concluded that, even if such value were present, the accused appropriator did not deprive them of value because, again, the plaintiffs handed it over in the first place.[2] This becomes even more problematic in the data collection context, because companies oftentimes digitally package the information they receive in ways that are only valuable to them.

Statutory Law

With respect to statutory law, a good example of how the law fails to recognize certain harms under a privacy claim involves the case of Stanmore Cawthan Cooper[3], a licensed pilot diagnosed with HIV who had disclosed his medical condition to the Social Security Administration (SSA) to collect disability benefits, under the reasonable belief that such health information would remain confidential. As part of an interagency crackdown on those who were fraudulently gathering disability benefits or those who lied on their, the SSA disclosed Cooper health information to the FAA and DOT. The Supreme Court held that the government violated the Privacy Act of 1974, but Cooper was denied damages for mental or emotional distress. The fact that the Court refers to the nature of the privacy harm as having a "chameleon-like" quality lends further evidence that courts in general suffer from this problem of concretization.

Regulatory Law

With respect to regulatory law, the Federal Trade Commission is the de facto enforcer of consumer privacy, which through Section 5 of the FTC Act, investigates and prohibits unfair and deceptive trade practices. However, for a practice to raise to the level of deceptiveness or unfairness necessary to trigger federal action, it must "be likely to cause substantial injury to consumers which is not *reasonably avoidable* by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[4] This is yet another example of viewing privacy and privacy harm as a balance test. In addition, this reflects thinking of privacy in terms of control, choice, and autonomy; that consumers are rational agents in control of making information sharing decisions. But it is difficult to accept this role of consumers when, every day, they are faced with products and services with terms of use that are far from transparent, which is troubling considering that transparency is one of the foundational fair information practice principles.

<u>The Fair Information Practice Principles (FIPPs)</u>

This section addresses problems with the proposal's description of the most foundational FIPPs." With respect to the proposal's sections on "security" and "control," the principles are frequently framed in terms of "user expectations" or what a consumer "should expect" from an organization with regard to the use of personal information. However, the proposal does not include recommendations for how the law can help enforce those expectations when organizations do not—again, perhaps as a means to avoid appearing overly prescriptive. Moreover, it does not address how data will be secured through any subsequent exchanging of hands[5]. For instance, the proposal states that "organizations should secure personal data at all stages, including… transfer."

---

[2] *Dwyer v. American Express*, 652 N.E. 2d 1351, 1356 (III. App. Ct. 1995)
[3] *Fed. Aviation Admin. v. Cooper,* 132 S.Ct. 1441 (2012)
[4] 15 U.S.C. § 45(n)
[5] Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 Stan. Tech. L. Rev. 431, 434 (2016)

In other words, the privacy outcome remains unclear as to how organizations ensure that third parties with whom they exchange data are themselves trustworthy and secure.

There are also a number of issues with respect to the proposal's description of "transparency." Firstly, the proposal requests that organizations inform consumers of how they "collect, store, use, and share" their consumers' personal information. This is nothing groundbreaking. Under the notice-and-choice regime, the mere act of adopting an openness with respect to notifying consumers about an organization's collection, use, and disclosure practices is typically enough to check off that organization's legal obligations to the detriment of consumers.[6] Secondly, the proposal seems to suggest that transparency hinges on consumers' "understanding" of such practices, which similarly implies that organizations can satisfy their obligation to protect consumer privacy once they have "informed" consumers. Thirdly, the proposal states that one way to achieve such understanding is to maximize the "intuitiveness" or user-friendliness of privacy policies, and briefly acknowledges that "lengthy notices" do not create understanding. However, neither shortening the length of a privacy policy nor increasing the overall utility or readability of a privacy policy will necessarily create transparency.

The notice and choice regime developed out of the notion that privacy is based on autonomy, choice, and control; that privacy is about the freedom to choose when and how to share personal information. So when organizations give us the "what-when-how" of data use practices, the idea is that consumers will be informed and, as a result, can make an informed decision about sharing their information. However, this framework is based on the "misconception that users make perfectly rational disclosure decisions[7]." Moreover, the choice to use an organization's products or services is seldom made freely or voluntarily, even after notification of information use practices. This is because the way in which information about an organization's practices is transmitted to consumers can manipulate consumers into harmful disclosures. In other words, design is arguably as important as the information itself.

Design

The proposal mentions "privacy-by-design" only once, and moreover, fails to explain the important role privacy-by-design, specifically the design of privacy policies, plays with respect to the protection of privacy. There are number of privacy issues that arise because of design. First, it is known that privacy policies are written in excessive legal jargon, such that the average user would experience great difficulty when trying to understand the terms contained within. This alone casts doubt on whether a "meeting of the minds" was actually achieved. But more troubling is the extent to which the aesthetic display of a policy can manipulate or deceive consumers into "volunteering" disclosures of personal information they might not have made had the policy been presented in less manipulative, less deceptive ways[8]. As law professor and scholar Ari Ezra Waldman argues, privacy policies are "written by lawyers and for lawyers."[9] He goes on to argue that, "by designing policies so no reasonable user could ever read, process, and understand them, drafters fail to provide adequate notice. This tactic is manipulative and unfair, arguably warranting regulation."[10]

On the matter of regulation, most federal regulatory action is triggered primarily when an organization makes a promise in its privacy policy and then breaks it. The problem with much of this "broken promise litigation" is that cases almost always end in settlement, and as a condition of settlement, the FTC requires organizations to include in their privacy policies certain substantive disclosures. In each case, the FTC virtually disregards[11] the unfair or deceptive nature of the design of the policies which manipulated or deceived users in

[6] *Id.* at 462
[7] Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 Stan. Tech. L. Rev. 74, 79 (2018)
[8] *Id.* at 79
[9] *Id.* at 79
[10] *Id.* at 80
[11] *Id.* at 89

the first instance.[12] For instance, in *In Re Sears Holding Management*, Sears misled consumers about its software, which when used began to collect swaths of data greatly inconsistent with the scope of collection disclosed in its policy.[13] But the FTC overlooked the fact that the agreement consisted of nineteen pages "of small print, with only a handful of subheadings."[14]

Under the notice and choice regime, the practice of focusing on the content of privacy to the neglect of design reflects a way of thinking about privacy solely in terms of autonomy; that consumers are viewed as rational agents capable of making their sharing decisions freely, without regard to the ways in which design can deceive and manipulate users as a means to manufacture consent. Waldman argues that, "by focusing almost exclusively on the content of privacy policies, notice and choice embeds an autonomy-based vision of privacy into the law."[15] Yet, as he reveals, by virtue of their design, privacy policies can "constrain user freedom and choice."[16]

B. Trust-Based Privacy Solutions: A Way to Fill What is Missing

Although the four torts of privacy have proven ill-equipped to offer redress to plaintiffs, there are ways of avoiding the concretization difficulties of privacy harm. One method would be to expand the definition of personally identifiable information (PII). For example, pieces of legislation like California's Online Privacy Protection Act (CalOPPA)[17] and the European Union's recent passage of the General Data Protection Regulation (GDPR) contain provisions that broaden the scope of the meaning of PII so that information that would not otherwise be viewed as "private" under the traditional privacy torts now could be. Furthermore, privacy harm can be conceptualized better if situated to some extent within the tort of breach of confidentiality, which is discussed further below.

Learning from Fiduciary Law

Certain scholars have advocated for adopting some of the principles of fiduciary law to help protect privacy and promote trust in interactions between consumers and organizations. Scholars Neil Richardson and Woodrow Hartzog have turned to the law of fiduciaries, which governs relationships defined by trust, to see how trust can be introduced specifically into the information relationships that abound in our age of ecommerce and social media, where so much of our financial and other personal information is transmitted across the Internet. Under their theory, trust works to the benefit of both consumers and organizations, or as they would call them, "trusters"[18] and "entrustees," because trust encourages a willingness to disclose in the first instance, despite the vulnerability that naturally attaches to disclosure, and untrustworthy businesses run the risk of consumers fleeing to more trustworthy competitors.[19]

The scholars argue that the law should treat organizations similarly to the way it treats doctors or financial advisors, with whom we entrust sensitive health and financial information.[20] We trust that these people will act in our best interest and not to reveal our health or financial information. So too we should be able to trust

[12] *Id*. at 89
[13] *Id.* at 89; Complaint at 1, *In re* Sears Holdings Mgmt. Corp., F.T.C. File No. 082 3099, No. C-Winter 4264 (Aug. 31, 2009) [hereinafter Sears Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf [https://perma.cc/BRZ9-56YG].
[14] *Id.* at 89; Exhibit E, Sears Complaint, https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscomplaintaf.pdf [https://perma.cc/3U2K-YCF7].
[15] *Id.* at 95
[16] *Id.* at 118
[17] Cal. Bus. & Prof. Code § 22575(b)
[18] Richards & Hartzog, *supra* note 5, at 450
[19] *Id,* at 465
[20] *Id,* at 433

organizations to handle our personal information with care, and not to our detriment. One way to promote such trust requires re-interpreting the FIPPs in trust protective ways.

Re-Interpreting the FIPs in Trust-Promoting, Privacy Protective Ways

Confidentiality

Richardson and Hartzog, among others, have argued that the tort of a breach of confidentiality provides a framework for rethinking about information relationships. Confidential relationships are those in which a person entrusts information in another, who as a result becomes a confidant prohibited from revealing that confidential information without the former's permission[21]. In the context of a search engine or online platform, this would entail an affirmative duty not to reveal our search history or purchase history[22]. It is important to note that the scholars admit that imposing a duty of confidentiality on every relationship would be too onerous, since at least in the consumer context, organizations need some degree of freedom to disclose the information that they acquire from users and customers[23]. Instead, they argue that the tort of confidentiality can be applied flexibly if re-envisioned as the imposition of a duty of "discretion." Organizations can act discreetly if "they can limit to whom they disclose information… what they share with others… and [if] they can control how they share information to make sure they preserve the trust placed in them."[24]

In terms of legally operationalizing this duty, Richardson and Hartzog propose a number of options. First, they argue for legislators to enact statutes to create a duty of discretion. Alternatively, they propose that the Federal Trade Commission's enforcement powers could be enhanced if, under certain circumstances, a finding of a lack of discretion fell within unfair or deceptive trade practices. They argue, "laws could look to whether entrustees made sure that recipients of data were trustworthy or whether they ensured that certain kinds of information were not publicly available through search engines like Google."[25]

Transparency

Because we have seen that consumers can still misinterpret what-when-how, privacy policies deemed sufficiently "transparent," under the proposal's description, it is important to identify how an understanding of privacy in terms of trust can supplement "transparency" in privacy protective ways. Richardson and Hartzog argue that for organizations to be truly transparent, they must have an "affirmative obligation of honesty to correct misinterpretations."[26] Indeed, they reimagine the FIP of transparency as understood to mean "honesty." The scholars even provide examples of how the law can force organizations to be more honest. For example, the California Online Privacy Protection Act (CalOPPA) requires every company that gathers information on Californians to provide consumers with notice and even mandates that those notices include specific disclosures of information use practices.[27] This statutory provision is sometimes referred to as a "mandatory disclosure regime."[28] Given California's huge economy, organizations have a large incentive to promote trust and comply

[21] Id, at 459
[22] Id, at 460
[23] id, at 459
[24] id, at 460
[25] id, at 462
[26] id, at 462
[27] Cal. Bus. & Prof. Code § 22575(b)
[28] Richards & Hartzog, *supra* note 5, at 464

with this law, lest they run the risk of losing customers—what Hartzog and Richards argued was the cost of untrustworthiness for organizations.

Security

In light of the ever-increasing frequency of data attacks and data breaches, Richardson and Hartzog argue that organizations must adopt a more "holistic"[29] approach to the fair information practice principle of security. They re-envision security as a "duty of protection"[30] and argue that organizations "must adopt a mentality of data stewardship, which includes protecting information passed on to others."[31] This seems to relate to the idea that privacy protection derives not only from protective laws and policies, but from the corporate ethos at large. Furthermore, the scholars recommend that organizations protect those features of data that are personally identifiable to the holder. As stated above, CalOPPA imposes a duty on operators of commercial websites or online services, with respect to their privacy policies, to "identify the categories of personally identifiable information" they collect.

Privacy Design

Research studies have shown that the design of privacy policies influences our behavior, namely our decisions on whether or not to trust websites, and thus, whether or not to share our personal information with them.[32] Based on his work, law professor and academic Ari Waldman argued that "inconsistent and confusing policy design was preventing consumers from becoming aware of their data privacy rights."[33] Consequently, and among other recommendations, Professor Waldman advocates that state and federal statutes, that require privacy policies, should additionally include policy design requirements that render policies more transparent.[34]

In addition, lawmakers can take a lesson from abroad, namely, the EU's recent passage of the General Data Protection Regulation, Article 25[35] of which concerns privacy design. The Article takes "cost of implementation" into consideration, a response to the concerns of some smaller companies and organizations, and perhaps the drafters of this proposal, who might fear the cost of implementing privacy protections in products and services. The Article imposes an obligation on entities to essentially ensure that their products or services are compliant with the data-protection principles recognized under the GDPR. Lastly, with respect to the obligation's time frame, the obligation is essentially active all the time, meaning entities must always consider how design can effectuate the data-protection principles. While the legislation is somewhat vague, American lawmakers could to certain extent base future legislature on its example.

[29] *id*, at 467
[30] *id,* at 436
[31] *id*, at 476
[32] Waldman, *supra* note 7, at 94
[33] *id*, at 94
[34] *id,* at 79
[35] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

Conclusion

In summation, this commentary began with a discussion of some of the principles missing from the proposal, including the idea that privacy harm is a harm, in addition to what was missing from the core principles mentioned. With respect to the former, lawmakers, courts, and companies will continue to face the problem of concretizing privacy harm if they do not change their thinking of what privacy means: less in terms of choice, control, and autonomy, and more so in terms of trust.

The second part of the discussion applies the re-interpretations of the FIPPs articulated by scholars Neil Richards and Woodrow Hartzog to supplement the privacy outcomes as they appeared in the NTIA's consumer privacy proposal. They based their theory similarly on the notion that privacy protections can be optimized through a change in perspective on what privacy means. This began with the scholars' arguments on how the tort of confidentiality can be adapted for privacy protection purposes in the context of information relationships. It then proceeded with transparency as honesty, and security as a duty of protection.

In addition, the discussion included recommendations by leading scholars on how the FTC's section 5 enforcement power could be made more robust if the scope of unfair and deceptive trade practices were broadened to include a lack of discretion and if they began to consider the impact design has on the ability of consumers both to freely make disclosure choices and to understand their data privacy rights.

Lastly, the commentary made mention of statutes like CalOPPA and the GDPRA, which represent examples of how future legislation can be written for more privacy protective outcomes.