To: National Telecommunications and Information Administration

From: Kia Mojabe

Date: November 9, 2018

RE: Request for Comments- Docket No. 180821780-8780-01

OUTCOME SEVEN- ACCOUNTABILITY

Introduction

While the seven outcomes provided by the National Telecommunications and Information Administration (NTIA) recognize necessary goals when approaching consumer data privacy, the outcomes are also broad.[1] In addressing question A(1) posed in the Request for Comments, the focus of this comment is on outcome seven: Organizations should be *accountable* for the use of personal data that has been collected, maintained or used by its systems.[2] Terms of this outcome need further explanation to fully understand it's meaning: who *organizations* are, what constitutes *use of personal data*, what constitutes *collection, maintenance, or use of systems*, and what constitutes *accountability*. While identifying the other terms is essential to understanding this outcome as a whole, the main focus of this comment is to address what constitutes accountability.

With the growth of technology, privacy law in the United States has often failed to hold organizations, such as companies and data collectors, accountable for their uses of personal data because it lacks comprehensive national privacy laws. Lack of accountability is shown by the need for national privacy laws and how other areas of law, specifically Tort and Contract Law, are ill-suited to provide redress. Plaintiffs with privacy claims find difficulty with two main issues: proving standing and identifying harm. The determination of this comment is to resolve these issues and demonstrate why it is time to create a national and uniform data protection regulation through information fiduciaries to protect individual privacy and resolve the differences between state and federal requirements.

Tort Law

Tort law once provided the most substantial protection for privacy; however, with the emergence of new technology, tort law has failed to provide redress for consumer privacy plaintiffs. Tort law protects individuals from another's civil wrongs against them. To succeed in

[1] National Telecommunications and Information Administration, *NTIA Seeks Comment on New Approach to Consumer Data Privacy*, (Sept. 25, 2018), https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy (last visited Nov 9, 2018).

[2] National Telecommunications and Information Administration, *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, (Sept. 25, 2018), https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf (last visited Nov 9, 2018).

any tort law claim, a plaintiff must show there is a duty owed by the defendant, the defendant breached that duty, the defendant caused the plaintiff's injuries, and the plaintiff should be awarded damages for those injuries.

While there are four privacy torts recognized, the privacy tort claims most often seen with data privacy are intrusion upon seclusion and public disclosure of private facts.[3] Plaintiffs have found difficulty proving elements necessary to a tort law claim, injury and actual damages. For example, a case with an intrusion upon seclusion claim demonstrates an issue courts find regardless of tort claim. In *Dwyer v. American Express*, the plaintiffs, American Express (AmEx) cardholders, sought to prevent AmEx from renting out cardholder information about cardholder spending habits to merchants of marketing programs.[4] The Court held AmEx did not invade consumer privacy when it collected and sold data about its cardholder's purchasing habits. [5] The Court explained that for a successful claim of intrusion upon seclusion, the intrusion must: (1) be unauthorized, (2) be offensive or objectionable to a reasonable person, (3) be an intrusion into a private matter, and (4) cause anguish and suffering. [6] The Court reasoned that the plaintiffs claim of intrusion upon seclusion failed because cardholders voluntarily gave information to American Express, which revealed a cardholder's spending habits and preferences. [7] American Express did not commit an unauthorized intrusion because it compiled voluntarily given information and its product of a compilation was rented out to others. [8] American Express created the value in the aggregate and the individual cardholder's information did not have value. Also, private financial information was not disclosed. [9] This court demonstrates that in tort law a company can collect and sell personal information to third parties without being held accountable because the harm of the plaintiffs is not recognized as harm.

Consent to give personal information is seen as approval to use it however a data collector likes. With the new ways in which our data is collected and the overwhelming trust that consumers have in the companies they provide personal information with, tort law no longer provides legal claims that can address the privacy harms of consumers today.

Power Imbalance

In today's information age, it is almost impossible to avoid using the internet from social ties of using Facebook or to shopping online with Target. Due to the inescapable reliance of the internet, individuals are vulnerable to organizations that they entrust personal data with because individuals need to participate in these spaces and do not have a legal system to hold

[3] Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1823, 1805-1825 (2010).
[4] *Dwyer v Am. Express Co.*, 273 Ill App 3d 742, 210 Ill Dec 375, 652 NE2d 1351 [1995].
[5] *Am. Express Co.*, 273 Ill App 3d at 742.
[6] *Id.* at 742.
[7] *Id.* at 742.
[8] *Id.* at 742.
[9] *Id.* at 742.

organizations accountable when they betray trust. Online experiences are almost entirely governed by algorithms, which makes protecting oneself from current technology nearly impossible for the average consumer. Large corporations act with authority because they have vast amounts of power over consumers and they are mostly self-regulating. Due to this power imbalance between consumer and data collector, federal actors have tried to take action.

Federal Regulation

In the United States, consumer protection regulation has had the broadest power to govern privacy and information security. In *Privacy and Data Protection Law,* William McGeveran describes today's privacy regulation. [10] The chief federal agency regulator is currently the Federal Trade Commission (FTC) whose role has grown because no other regulator has clear authority in this area, notwithstanding companies have pushed back on the FTC's authority. [11] Working alongside the FTC are state attorneys general and agencies. [12]

Under Section 5 of the FTC Act, the FTC asserts authority to govern data privacy by prohibiting companies from performing "unfair or deceptive acts or practices."[13] On its face, Section 5 does not confer the FTC with the power to impose monetary penalties. McGeveran states, "The FTC may pursue disgorgement of profits or restitution where the facts show clear financial harm- such as ordinary fraud cases brought under Section 5- but in most privacy cases, they do not." [14] There are other statues that can confer authority for the FTC to enforce privacy law through fines, but Section 5 grants the power to enforce equitable forms of relief. [15] The FTC has increased this broad authority aggressively with investigations on these "unfair" or "deceptive" practices in cases alleging website owners engaged in deceptive acts in failing to adhere to their privacy policies under notice and choice.

Notice and Choice

Today's privacy regime is largely governed by notice and choice, which appears in federal and state law. In *Privacy as Trust,* Ari Ezra Waldman describes when notice and choice was created, what it is, and why it fails to protect consumers.[16] In 1973, notice and choice emerged from a report by the federal Department of Housing, Education, and Welfare (HEW). [17] Notice explains when data collectors are required to describe data use practices, such as what

[10] William McGeveran, *Consumer Protection*, in Privacy and Data Protection Law 205-206 (2016). This comment recognizes the Department of Commerce's interest in privacy regulation since the early 1900s and 2000s.
[11] *Id*. at 205.
[12] *Id*. at 205.
[13] (15 U.S.C. Sec. 45(a)(1)).
[14] *Id*. at 206.
[15] *Id*. at 206.
16 Ari Ezra Waldman, *The Responsibilities of Data Collectors*, in Privacy as Trust: Information Privacy for an Information Age 80, 79–92 (2018).

[17] *Id*. at 80.

information they collect, how and for what purpose they collect it, and how they share it.[18] Choice describes the opportunity for individual users to consent to the collection of their data.[19] If users do not consent to these practices, then users can use other platforms.[20] After a user consents, this user has given an organization permission to use personal data given in accordance with the privacy policy made by that organization. The FTC undertook notice and choice and applied these standards to commercial websites, which affected privacy policies. [21]

Some industries are required by statute to disclose privacy policies, such as actors in health care industry through the Healthy Insurance Portability and Accountability Act (HIPPA).[22] However, companies, like Amazon or Facebook, are not required to provide privacy policies because there are no national industry specific statutes that require them to disclose privacy policies, making notice and choice under-inclusive. [23] Companies can disclose privacy policies, usually to make consumers trust in their data use practices, without regulations and develop their own standards and practices about privacy.

Federal regulation to ensure these companies abide by the data use practices embellished in their privacy policies has been done by the FTC's enforcement action of ensuring adequate notice. In *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, Jennifer Woods explains, "The majority of the FTC's privacy and data security cases involve the "deception" prong…Many cases are not based solely on Section 5, and instead include violations of other related statutes…no court has ruled on the FTC's interpretation of the scope of its authority under the "unfairness" prong…"[24] These enforcement actions have shown to be inadequate.

Moreover, notice presents issues because consumers ordinarily do not read or understand a company's privacy policy. In *What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It*, Joseph Turow explains, "64% [of the people surveyed] do not know that a supermarket is allowed to sell other companies information about what they buy" and 75% falsely believe that when "a website has a privacy policy, it means the site will not

[18] *Id*. at 80.
[19] *Id*. at 80.
[20] *Id*. at 80.
[21] *Id*. at 80-84.
[22] *Id*. at 80-84.
[23] *Id*. at 80-84.
[24] Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5,* ABA Young Lawyers Division Publications Blog, (March 26, 2013), https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy/.

share my information with other websites and companies."[25] Moreover, Lorrie Faith Cranor conducted a study that showed it would take an individual an average of 244 hours per year to read a privacy policy of all the websites she visited.[26] Further, privacy policies can be changed as often as the website operator would like, making it difficult for users to know when to reread a policy.

Additionally, Waldman explains choice fails because it does not account for consumer privacy expectations.[27] It would become cumbersome to interact online, especially when most of our interactions are for convenience, if consumers had to constantly reevaluate their privacy preferences.

Most importantly, notice and choice fails because it does not fully protect consumers against today's technology or privacy harm. As seen in *Dwyer v. American Express,* big data algorithms are made to create personally identifiable information from the collection of its users and the way companies use this data will not be disclosed. [28]

In conclusion, notice and choice as a concept fails largely because of how consumers interact online and how technology has evolved; moreover, when privacy policies are challenged in practice, other areas of law cannot hold their owners accountable either.

Contract Law

Plaintiffs, who have filed claims against data collectors for not abiding by their privacy policies, have found difficultly using contract law to remedy their harm because of the obstacle of establishing the existence of a contract, an essential element to determining a breach of contract claim.

In *In re Northwest Airlines Privacy Litigation*, under a breach of contract claim, plaintiffs claimed Northwest violated its privacy policy from its website that provided Northwest would not share a customers' information unless it was necessary to make a customers' travel arrangements when Northwest provided customer information to the National Aeronautical and Space Administration (NASA) for security purposes.[29] The Court held plaintiffs failed to allege an essential element of a contract claim, acceptance of the offer; further, even if a contract were

---

[25] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 596 (2014). (using data from Joesh Turow) Joseph Turow et al., *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* 21 (Sept. 29, 2009).

[26] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* 4 I/S 543, 563 (2008).
[27] Waldman, supra note 22, at 84.
[28] *Id*. at 84-85. Also, *Am. Express Co.*, 273 Ill App 3d at 742.
[29] *In re Nw. Airlines Privacy Litig.*, No. 04-126 (PAM/JSM), 2004 U.S. Dist. LEXIS 10580 (D. Minn. June 6, 2004).

found, the plaintiff failed to allege any contractual damages from the alleged breach. [30] Requirements of a valid contract include: offer, consideration, acceptance, and mutuality.[31] The Court reasoned that since the plaintiffs did not show they read the privacy statement, the plaintiffs failed to show they accepted the offer; therefore, not showing mutuality or a "meeting of the minds," when both parties have the same understanding of and both agree to the terms of a contract at the same time. [32] Thus, the Court found the privacy statement was not a valid contract as the plaintiffs did not show the essential element of accepting the offer. [33] Moreover, the Court mentioned even if it found the policy statement to be a contract, the plaintiffs failed to allege any contractual damages. [34] This case provides an example of how many courts have not found privacy policies to fall within contract law. However, not all courts have agreed with the court in *Northwest*. [35]

Some courts have found privacy policies are contracts, likely contracts of adhesion, which are contracts drafted by one party who usually has stronger bargaining power and signed by another who usually has weaker bargaining power. Due to notice and choice, these contracts are valid because individuals have the choice as to whether to use a specific website. In *In re JetBlue Airways Corp. Privacy Litigation*, the plaintiffs alleged that the defendant, JetBlue Airways Corporation, failed to comply with their privacy policy that stated JetBlue would not share passenger information with third parties when JetBlue provided personal information to a third party.[36] JetBlue gathered and kept personal information of its passengers in the Passenger Name Records (PNRs), that included passenger's addresses, telephone numbers, and flight itineraries, which passengers provided when purchasing flights. [37] The Court held that the plaintiffs' claims of breach of contract from JetBlue's failure to comply with its privacy policy was without merit because the plaintiffs did not prove the existence of damages.[38] This court recognized the *Northwest* court had a narrow reading of acceptance and viewed these plaintiffs to have accepted the offer when they relied on the statements from the policy as it is difficult to determine which plaintiffs actually read the policy. [39] To succeed on a breach of contract claim, the plaintiff must show an existence of damages. The Court reasoned the plaintiffs did not prove damages because the only harm alleged is loss of privacy and this loss is not a recoverable damage in a breach of contract case since solely economic damages from a breach are

[30] *In Re Northwest Airlines Privacy Litigaton*, No. 04-126 (PAM/JSM) at 10580.
[31] *Id.* at 10580.
[32] *Id.* at 10580.
[33] *Id.* at 10580.
[34] *Id.* at 10580.
[35] *Id.* at 10580.
[36] *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

[37] *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d at 299.

[38] *Id.* at 299.
[39] *Id.* at 299.

recoverable.[40] Thus, this decision highlights another reason how an area of law fails to keep organizations, like JetBlue, accountable when using consumer personal data.

Regardless of whether a contract is found, the issue of privacy harm as a harm was seen as both courts struggled to address awarding damages. Both courts show the viability of contract claims alleging privacy policy violations as rare. In conclusion, the overarching issues seen in tort law are the same in contract law. Standing is an issue as courts have found that privacy policies are not contracts and would thus not be governed by contract law. On the other hand, privacy harm is not defined and leaves courts unable to award damages.

Fiduciary Law

Created through common law, Fiduciary Law imposes legal duties on particular individuals in society. In *Privacy as Trust*, Ari Ezra Waldman explains fiduciary law focuses on relationships of trust and there is an obligation of loyalty.[41] Examples of information fiduciaries include: lawyers, doctors, and investment advisers.[42] A client puts his or her trust in a fiduciary, and the fiduciary has an obligation not to betray that trust by acting in the client's best interest and not in a way that is harmful to the client.[43] Accountability is ensured because if a fiduciary breaches their duty to put the client's best interests first, then they will have breached a duty recognized and remedied through tort law.

Organizations should be held to greater accountability than notice and should be fiduciaries to personal data. Waldman provides four reasons why data collectors should be considered information fiduciaries.[44] First, consumers are vulnerable to companies. Waldman states, "They know everything about us…trade secrecy keeps their algorithms hidden from us."[45] Second, users are dependent on these companies because many of us cannot live in today's world without acting on these platforms. [46] Third, these companies' market as the best for that service, which causes consumers to only use that provider. [47] Fourth, these companies take significant efforts to appear trustworthy. [48] For these reasons, consumers are fated to live in a world where data collectors control how they use personal data and are not held accountable for when they misuse it.

Fiduciary law could recognize privacy harm is a harm and could provide a way to hold companies accountable. In *Reforming the U.S. Approach to Data Protection and Privacy*, Nuala O'Connor explains how the U.S. legal framework should recognize means to understand privacy

[40] *Id.* at 299.
[41] Waldman, supra note 22, at 84.
[42] *Id.* at 85.
[43] *Id.* at 85.
[44] *Id.* at 86-87.
[45] *Id.* at 86-87.
[46] *Id.* at 86-87.
[47] *Id.* at 86-87.
[48] *Id.* at 86-87.

harm as privacy harm. [49] O'Connor states, "These less quantifiable harms that result from the exposure of bits and bytes of individuals' personal lives should be recognized by law: as the depts of these harms are plumbed and addressed over time, individuals should be afforded a private right of action to hold companies accountable, and regulators should have the ability to penalize entities that flout their duty to be responsible stewards of personal information."[50] O'Connor references Jack Balkin to explain how information fiduciaries could ensure privacy harms are recognizable legal harms. [51]

In *A Grand Bargain to Make Tech Companies Trustworthy*, Jack M. Balkin & Jonathan Zittrain explain information fiduciaries can be applied in practice by what they propose to be a grand bargain.[52] They propose a duty of care for personal information would be expected of data collectors in exchange for legal clarity and safe harbors for specific industries. This proposal would be in the form of a federal statute and would preempt state and federal privacy laws. To elaborate, Waldman describes how a regime of information fiduciaries would embolden the FTC. He states information fiduciaries in a regime of understanding privacy as privacy as trust "would give the agency a doctrinal foundation for including inducement of misplaced trust as a "deceptive business practice" under Section 5 of the FTC Act."[53] The FTC, or any other agency such as the NTIA, could gain the statutory authority it needs by embodying the concept of information fiduciaries.

Restructuring the legal system from notice and choice and understanding that privacy policies seen in Tort and Contract Law does not hold organizations accountable, fiduciary law could help solve the power imbalance between data collectors and consumers and could ensure data collectors are held accountable. Under the theory of information fiduciaries, privacy victims could have standing if there is a specific duty data collectors owe to consumers; moreover, privacy harm would be a harm recognized by law.

Conclusion

The NTIA is concerned with stifling flexibility to innovate and might fear regulation. However, technology regarding personal data is evolving faster than the law can understand how to regulate it. User reliance on technology will inevitably catch up to consumers' detriments and the United States will fall behind to other countries that have national privacy laws. If accountability, as was shown through our current regime and Tort and Contract Law, is not practiced, consumers will begin to lose trust in data collectors and this could stifle innovation in

[49] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy,* (2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

[50] O'Connor, supra note 48.

[51] *Id.*

[52] Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy,* ATLANTIC (Oct. 3, 2016), www.theatlantic.co/m/technology/archive/2016/10/information-fiduciary/502346.

[53] Waldman, supra note 22, at 89.

consumer America further. Due to these reasons, data collectors should be information fiduciaries recognized nationally.

Word Count: 2992