Katelyn James
J.D. Candidate at New York Law School

INTRODUCTION

This memo addresses two outcomes that should be included in any federal legislation on consumer data privacy: (1) establishing online service providers[1] as information fiduciaries and (2) authorizing state attorneys general to enforce federal legislation on their citizen's behalf. By including these two approaches, many user-centric privacy outcomes identified by the NTIA can be achieved, including transparency, accountability and harmonization while balancing current business practices.[2]

I. INFORMATION FIDUCIARIES

Fiduciaries are parties that have a relationship of trust with their clients, and are authorized to manage the property or assets on their behalf.[3] Fiduciaries owe several duties to their clients, such as acting with duties of care and loyalty.[4] Information fiduciaries such as lawyers, doctors and accountants are already recognized under the law, and have access to their client's personal and sensitive information.[5]

Online service providers have taken on the role of information fiduciaries through the collection and use of personal information.[6] Like traditional information fiduciaries, online

[1] For the purpose of this memo, online service providers includes any online business or service that collects, uses, analyzes or sells personal data.
[2] NTIA, "Developing the Administration's Approach to Consumer Privacy," (Notice for Public Comments) 83 Fed. Reg. No. 187 (2018), https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf
[3] Jack M. Balkin, *Information Fiduciaries in the Digital Age,* BALKINIZATION (Mar. 5, 2014), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html
[4] A duty of care includes acting in the best interest of the party. A duty of loyalty includes avoiding conflicts of self-dealing and may include a duty to disclose how assets are being managed. *Id.*
[5] They also operate under a duty of confidentiality, and relationships of trust are central with the use and sharing of personal and sensitive information. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 at 1208 (2016)
[6] *Id.* at 1221

service providers have economic relationships[7] with users[8] based on asymmetrical power because they collect sensitive information that can be used to manipulate or discriminate against users.[9] Users are dependent on the services provided,[10] and because there are a few companies that dominate the online market,[11] users have little, if any, choice to use other platforms.[12] Similar to traditional information fiduciaries, online service providers possess knowledge and expertise users do not have.[13] They may also set themselves up as being trustworthy with our sensitive information,[14] even though they do not always act in trustworthy ways.[15]

Traditional information fiduciaries have enforcement mechanisms, including licensing boards and malpractice insurance[16] and lawsuits are brought against them if they breach their fiduciary duties.[17] Establishing online service providers as information fiduciaries is a strong way to enhance consumer data privacy because it protects consumers, evidenced by traditional

[7] Adam Schwartz & Cindy Cohn, *"Information Fiduciaries" Must Protect Your Data Privacy,* ELECTRONIC FRONTIER FOUND. (Oct. 25, 2018), https://www.eff.org/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy

[8] This framework is presented as applying to users, but it should also apply to employees of online service providers. Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations,* 33 BERKELEY TECH. L. J. 1 at 17, 22 (2018)

[9] Users expect a "fair shake" with the information they are given, such as how to do something or get somewhere. *See* Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARVARD BUSINESS REVIEW (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for

[10] Balkin, *supra* note 5 at 1222

[11] Rachel Wilka, *Privacy Commitments,* 93 WASH. L. REV. 63 at 71 (2018) citing Jeff Desjardins, *This Chart Reveals Google's True Dominance over the Web,* VISUAL CAPITALIST (Apr. 20, 2018), http://www.visualcapitalist.com/this-chart-reveals-googles-true-dominance-over-the-web/

[12] Individuals should be encouraged to use online services that makes life easier without their data being abused. Balkin, *supra* note 5 at 1223

[13] Examples include matching services such as ride-hailing applications, dating sites and search engines. *Id.* at1222

[14] *Id.*

[15] The FTC brought an enforcement action against Snapchat for its deceptive design that compromised privacy without user knowledge. *See* Ari Ezra Waldman, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 88-90 (2018). In 2018, the FTC settled with Venmo for its misleading privacy policies. *See also* Sarah Perez, *The FTC Settles with Venmo over a Series of Privacy and Security Violations,* TECHCRUNCH *(*Feb. 27, 2018), https://techcrunch.com/2018/02/27/the-ftc-settles-with-venmo-over-a-series-of-privacy-and-security-violations/

[16] Balkin, *supra* note 3

[17] Schwartz & Cohn, *supra* note 7

information fiduciaries that have legal obligations to keep our information private,[18] without "heavy-handed" regulation.[19] Recent state laws, such as the California Consumer Privacy Act, have taken steps towards the information fiduciary model with provisions including disclosure about data being collected,[20] where data is being sold,[21] and data minimization requirements.[22] This trajectory towards an information fiduciary approach should continue by codifying the relationship between users and online service providers under federal law.

II. INFORMATION FIDUCIARY PRINCIPLES

When determining who should be considered an information fiduciary, the law should consider: (1) an online service provider that collects, uses, sells, analyzes or transfers data that is recognized as personal data[23] (2) the number of people whose data it collects[24] and (3) revenue that is generated from the use of data[25] as not all companies that operate on the internet should be considered information fiduciaries.[26]

The government can protect the information that is obtained through reasonable regulation.[27] The duties of an information fiduciary should consider the obligations that

[18] Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/
[19] Imposing information fiduciaries has bipartisan appeal because it combines consumer protection with less federal regulation. Zittrain, *supra* note 9
[20] CALIFORNIA CONSUMER PRIVACY ACT OF 2018, §1798.100(a), §1798.110 and §1798.115
[21] *Id.*§1798.115(a)(2)
[22] *Id.*§1798.100(b)
[23] Any federal statute has to clearly define personal data. Article 4 of the GDPR defines personal data as any information relating to an identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
[24] Dobkin, *supra* note 8 at 47
[25] Adam Schwartz, Corynne McSherry, India McKinney & Lee Tien, *New Rules to Protect Data Privacy: Where to Focus, What to Avoid*, ELECTRONIC FRONTIER FOUND. (July 2, 2018), https://www.eff.org/deeplinks/2018/07/new-rules-protect-data-privacy-where-focus-what-avoid
[26] Balkin, *supra* note 3
[27] Balkin, *supra* note 5 at 1205

traditional information fiduciaries must uphold[28] as well as: (1) the kind of services provided,[29] (2) type of data collected[30] and (3) user expectations.[31] Most importantly, under an information fiduciary approach, online service providers would agree not to use personal data that discriminates against users or violates user trust when they reasonably expect their information to be protected.[32] Some of the duties should include:

1. Duty of Loyalty: Information fiduciaries would owe a duty act in the best interest of its users before its own self-interest, including not using data for different purposes or for exploitative reasons,[33] a duty to disclose the use of personal data[34] and a duty to disclose data breaches.[35]
2. Duty of Care: Information fiduciaries would owe a duty to act in the best interest of data management,[36] including taking affirmative action to secure personal information. This includes more than preventing security breaches[37] but owing a

[28] Robert A. Kutcher, *Breach of Fiduciary Duties* in BUSINESS TORTS LITIGATION, 4-10 (2005)
[29] For example, services that provide information users rely on, such as search engines, location services and social platforms which may influence user behavior should have different duties than services that merely conduct single transactions.
[30] Examples include personal information and location data.
[31] Duties should arise based on user expectations of the platforms, either established by the platform in their privacy policy or based on the type of services it provides. For example, users do not expect platforms to read their emails and messages and then advertise to the user based on their conversations, but might expect advertisements based on previous purchases.
[32] Balkin & Zittrain, *supra* note 18
[33] Behavior that should be curtailed by information fiduciary law includes manipulation, discrimination, third party sharing and violating privacy policies. Dobkin, *supra* note 8 at 17. Discrimination of data includes using race or gender to prevent access to certain products or advertisements. *Id.* at 26-32. It can also include using quiz results to influence voting or directing users on a route that passes an establishment because they paid the online service provider. Schwartz & Cohn *supra* note 7. It would also prevent predatory advertising such as payday loans. Zittrain *supra* note 9
[34] Schwartz & Cohn, *supra* note 7
[35] There is no federal law requiring data breach notifications, expect in certain sectors such as such as healthcare providers and financial institutions. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583 at 587 (2014)
[36] We should not expect digital companies to tell us how to use their platforms. The duty would be limited as compared to other traditional information fiduciaries. Balkin, *supra* note 5 at 1228-1229.
[37] *Id.*

duty of care with how data is stored and sold to third parties.[38] This should include verifying third party companies where data is sold is adhering to the same privacy requirements as the original data collector.[39]

III. JUSTIFICATIONS FOR INFORMATION FIDUCIARIES

Considering personal data is the most important revenue source for many online service providers,[40] under an information fiduciary approach, business practices can continue, but they cannot include using personal data in way that that violate user trust in exchange of free services.[41] As online service providers grow and expand, so do the uses of personal data. Imposing fiduciary duties is a more flexible approach to consumer privacy because imposes little cost to comply as long as they are not betraying users and can be adjusted upon changes in data use. By conceiving an information fiduciary standard, several of the user-centric privacy outcomes proposed by the NTIA can be achieved, such as transparency, reasonable minimization, risk management, accountability and harmonization.

1. TRANSPARENCY[42]

Information fiduciaries can achieve the privacy outcome of transparency because it requires online service providers to disclose how data is being used.[43] The federal law should consider balancing disclosure with the need for companies to keep some information private to prevent hacks and for trade secrets.[44] Some suggestions include: (1) hiring and consulting with data privacy specialists to determine what information should be disclosed and how (2)

[38] Dobkin, *supra* note 8 at 38
[39] Waldman, *supra* note 15 at 88
[40] Balkin, *supra* note 5 at 1226
[41] Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act*: Hearing Before the S. Comm. on Com., Sci.& Transp.* 115th Cong. (2018) (statement of Laura Moy, Executive Director, Center on Privacy & Technology at Georgetown Law)
[42] NTIA, *supra* note 2
[43] Balkin, *supra* note 3
[44] Balkin, *supra* note 5 at 1223

determining when data regulation should occur given that most personally identifiable information is not created at the time of collection or transfer[45] (3) comprehensible policy summaries of data practices[46] (4) public audits on how data is used and transferred[47] and (5) an option for users to filter content without the use of personalized information.[48]

Imposing fiduciary duties will benefit current business practices because it will cultivate more information sharing.[49] If individuals know their data will not be abused, they are more likely to share information they may have previously withheld,[50] making products and services better with more user input.

2. REASONABLE MINIMIZATION[51]

Creating an information fiduciary standard will impose the duty to ensure data collection is reasonable in the context collected in order to act in the best interest of the user. If the use of data exceeds the purpose it is collected for or has not been consented to, an online service provider would be in violation of its fiduciary duties. Additionally, fiduciary duties can help achieve the goal of data minimization because companies need to consider the best interests of their users when determining what data they need to store and for what purpose, as the indefinite storage of large amounts of data poses risks of data loss and breach.[52] It would violate fiduciary duties if information is leaked, especially if that information was not needed for any reasonable

[45] Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 at 106 (2014)
[46] Dobkin, *supra* note 8 at 49
[47] Balkin & Zittrain, *supra* note 18
[48] *Id.*
[49] Waldman, *supra* note 15 at 88
[50] *Id.*
[51] NTIA, *supra* note 2
[52] Bernard Marr, *Why Data Minimization is an Important Concept in the Age of Big Data*, FORBES (May 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#11e4403b1da4

purpose. Considering the GDPR[53] and the California Consumer Privacy Act[54] have provisions on data minimization, imposing fiduciary duties will help keep online service providers in compliance with data minimization principles imposed elsewhere.

3. RISK MANAGEMENT[55]

There are many ways under an information fiduciary approach to mitigate the risk of data exposure while upholding current business practices. This can include sharing data in an aggregated format, where no individual can be identified.[56] Online service providers can still aggregate data to identify products and behavior that is common in users, as long as it does not discriminate or manipulate users.[57] There are also alternatives for current targeted advertising, such as having the online service provider identify targets rather than sharing user information with third parties.[58] This can decrease the risk information shared will be used to discriminate or be used in ways users have not consented to by third parties[59] as many users do not know any information about the third parties who receive their information and what they do with the data.[60]

4. ACCOUNTABILITY[61]

Currently, there are federal and common law provisions that provide individual causes of action for privacy violations. Under the federal law, there is the Electronic Communications Privacy Act of 1986, which includes provisions such as the Wiretap Act and the Stored

[53] GDPR Art. 5
[54] *Id.*§1798.100(b)
[55] *Id.*
[56] Dobkin, *supra* note 8 at 40
[57] *Id.*
[58] *Id.*
[59] Additional risk management tools may include suggesting the FTC require more transparency for native advertising on platforms such as Facebook. *See* Waldman, *supra* note 15 at 92
[60] *Id.* at 87
[61] NTIA, *supra* note 2

Communications Act.[62] The Second Restatement of Torts recognizes privacy violations in claims such as intrusion upon seclusion,[63] public disclosure of private facts,[64] and in limited circumstances, breach of confidentiality.[65] However, successfully pursuing these torts claims are often challenging for individuals, as courts have dismissed cases for failure to show injury and because they held the information users voluntary gave to companies was no longer private.[66] Under contract law, many plaintiffs face similar challenges proving damages, and courts have held privacy policies are not enforceable contracts.[67] There is also no private cause of action under the Section 5 of the FTC for users who may be victims of "unfair and deceptive" trade practices by online service providers.[68]

Imposing information fiduciaries will hold online service providers more accountable because it will owe its fiduciary duties to users as well as its own privacy policies, where user expectations may arise.[69] Under a fiduciary approach, accountability is also increased by granting individuals the ability to bring a private cause of action in situations other than data breaches, as violations of fiduciary duties does not need to include data breaches.[70] By establishing information fiduciaries, harmful practices such as using data to discriminate users based on race or gender will be barred as a violation of a fiduciary duty.[71] Individuals will now have more opportunity to hold companies accountable, and will not have to rely on tort or contract law to bring claims if there are established duties that have been violated.

---

[62] 18 U.S.C § 2510-22
[63] Restatement (Second) of Torts §652 (b) (1965)
[64] *Id.* §652 (d)
[65] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, at 157 (2007)
[66] Dwyer v. American Express Co. 652 N.E.2d 1351 (1995); Shibley v. Time, Inc., 45 Ohio App 2d 69 (1975)
[67] Dyer v. Northwest Airlines Corps., 334 F. Supp. 2d 1996 (D.N.D. 2004)
[68] Solove & Hartzog, *supra* note 35 at 610
[69] Dobkin, *supra* note 8 at 45
[70] §1798.150 (a)(1) limits the ability for a private cause of action for only certain data breaches. Under §1798. 155 (a), an AG can bring a suit against companies that violate any parts of the act.
[71] Dobkin, *supra* note 8 at 26-32

5. HARMONIZATION[72]

Several proponents of the information fiduciary approach argue that in return for taking on new duties, the government should preempt online service providers from certain privacy laws, including existing and future state regulation.[73] However, federal law should not preempt existing state laws to achieve the goal of harmonization because it would eliminate certain privacy protections with its broader provisions.[74] These would preempt state privacy laws that have been codified and relied upon, and cause many local matters to become overlooked.[75]

Companies such as Apple are already complying with new laws such as the GDPR, and are starting to bring these protections to users in the United States.[76] Compliance in federal and state regulation will not preclude new innovation, as many new companies can hire compliance officers and lawyers to assist them.[77] Like compliance with employment law and OSHA regulations, upholding data privacy protections is a cost of doing business in the digital age. Imposing the fiduciary relationship should not allow for online service providers to be exempt from other laws that may provide additional privacy protections, such as control, access and correction.[78] Imposing fiduciary duties on companies is a fair way to balance current business models that use personal data in exchange for the promise it will not be misused.

[72] NTIA, *supra* note 2
[73] Balkin & Zittrain, *supra* note 18
[74] Gennie Gebhart, *EFF Opposes Industry Efforts to Have Congress Roll Back State Privacy Protections,* ELECTRONIC FRONTIER FOUND. (Sept. 24, 2018), https://www.eff.org/deeplinks/2018/09/eff-opposes-federal-preemption-state-privacy-laws
[75] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 at 799 (2016)
[76] Michael Grothaus, *Now You Can Easily See Exactly What Apple Knows About You*, FAST COMPANY (Oct. 17, 2018), https://www.fastcompany.com/90252274/now-you-can-easily-see-exactly-what-apple-knows-about-you
[77] Citron, *supra* note 75 at 802
[78] NTIA, *supra* note 2

6. SCALABILITY[79]

Additionally, information fiduciaries can help achieve the goal of scalability by providing an exception for companies that are small in terms of revenue, amount of users and data use.[80] However, the statute should be clear not to exempt online service providers from being fiduciaries if it handles sensitive information and holds itself out to be trustworthy. By establishing the principles of information fiduciaries, the law has flexibility to determine the scope of its application. If the fiduciary principles are created based on the nature of the business, the data it collects and user expectations, it provides an fair approach to federal regulation that will not overburden small companies while still enforcing data privacy protections against those who benefit from the use of personal data.

IV. ENFORCEMENT BY ATTORNEYS GENERAL

Any federal regulation on consumer data privacy, regardless of its scope, will put a strain on the FTC's enforcement ability. Currently, the FTC has a "common law" approach to privacy given it does not have traditional rule making abilities.[81] The FTC frequently settles and the consent decrees given to companies with large data breaches often provides a pass for admitting wrongful behavior.[82]

Additional enforcement mechanisms should include granting attorneys general the ability to bring claims under the federal statute on behalf of their citizens. State attorneys general have argued for more consumer protection, and have been on the "front-line"[83] of privacy enforcement

[79] *Id.*
[80] Dobkin, *supra* note 8 at 47
[81] Solove & Hartzog, *supra* note 35 at 586
[82] *Id.* at 610
[83] Citron, *supra* note 75 at 780

for the past fifteen years,[84] establishing and enforcing privacy norms.[85] Attorneys general also enforce other federal statutes, such as HIPAA violations, as the Department of Health and Human Services was unable to enforce them all[86] and their authority should be extended to include claims under any new federal legislation for consumer privacy.

Imposing the authority of attorneys general to enforce the federal law can also can help achieve the goal of harmonization.[87] Many attorneys general are currently working to maintain compliance with European law including data breach notification norms, providing privacy policies in understandable ways and protections for sensitive information.[88] They can help harmonize existing state laws to find the best approaches to create a more "homogenous" approach to privacy law, and many attorneys general have emphasized harmonization as a shared goal.[89]

The federal statute must provide the ability for the FTC to enforce the law in a way that is clear to the user and to the online service provider,[90] and granting attorneys general enforcement authority will help uphold the standards of the statue by providing additional enforcement opportunities for individuals. The federal statute should consider the common law rules of fiduciaries for guidance on how to enforce these standards[91] and how attorneys general can bring claims when online service providers breach their fiduciary duties.[92]

---

[84] *Id.* at 748
[85] *Id.* at 785
[86] *Id.* at 799
[87] NTIA, *supra* note 2
[88] Citron, *supra* note 75 at 795
[89] *Id. at 802*
[90] Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act*: Hearing Before the S. Comm. on Com., Sci.& Transp.* 115th Cong. (2018) (statement of Nuala O'Connor, President & CEO, Center for Democracy & Technology)
[91] Fiduciary breaches may arise out of a contract, but courts have enforced tort duties not explicitly agreed to by the parties and award damages. Balkin, *supra* note 5 at 1206
[92] Kutcher, *supra* note 28

CONCLUSION

If we treat online service providers that gather and collect personal data as information fiduciaries, we can help achieve the balance between consumer data privacy and current business models because companies that currently use personal data can still make a profit without abusing users trust, allowing for innovation and protection.[93] Empowering state attorneys general to bring claims will also help with the enforcement of any new data privacy protection without overburdening the FTC, giving citizens more opportunities to bring claims and be heard.

[93] Balkin, *supra* note 3