I. Introduction:

The proposed high-level goals and principle-based privacy outcomes sought in the Request for Comments are laudable ideas focused to safeguard the future of privacy law in America. As a current student of law, I am thankful for the opportunity to comment on one of the most interesting and salient areas in both law and society today.

Almost 130 years ago, Justices Warren and Brandeis famously recounted the evolution of the law's remedies.[1] They began by describing when the law sought to remedy primarily physical harms, and continued to the current time they wrote the article, where the law was just beginning to remedy intangible harms.[2] Additionally, the Justices observed how new innovations called for new and innovative legal remedies.[3] We are again at such a point of evolution in society and technology. Therefore, the law must evolve to address the new problems of the day, particularly in privacy law.

Below I will contend that the current notice-and-choice regime in privacy law inadequately addresses several problems in consumer privacy and comes short of fulfilling many goals requested in the Request for Comment. Within this argument, I will explain what a privacy-as-trust regime is and how it can better achieve the various privacy outcomes and high-level goals than a notice-and-choice regime could. Next, I will explain the importance of design and why conceptions of autonomy in privacy law may be detrimental to implementing a cogent privacy law regime. Then, I will state how a privacy-as-trust regime is compatible with Federal Trade Commission enforcement. Finally, I will point out what consumer privacy can learn from Fourth Amendment jurisprudence.

II. The Problems with Notice-and-Choice

As stated in the Request for Comments, the current notice-and-choice regime in privacy law results in long, legalese-filled privacy policies that are seldom read by users. As a result of this notice-and-choice regime, many users make poor decisions in regard to their privacy. This is because of the stark size of privacy policies, as well as their difficulty to read and understand.[4] What is more, underlying societal pressures render choice meaningless in several ways.[5] For example, social media and smart phone use are both virtually indispensable in regard to living in today's society. Because of their indispensability, abstaining from using them becomes effectively impossible. This is true regardless of what lies in their long, complex privacy policies.[6] Thus, choice is rendered meaningless in such circumstances.

Furthermore, companies that participate in information gathering largely tout their trustworthiness. This is achieved in various ways. For example, many companies emphasize the amount of people who use their platform in ads. This induces trust in users toward the platform since users recognize large numbers of users to be an indication of trustworthiness.[7]

---

[1] Samuel D Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. (1890).
[2] *Id.* at 192-96.
[3] *Id.* at 206.
[4] Ari Ezra Waldman, PRIVACY AS TRUST 84 (2018).
[5] *Id.* at 66.
[6] *Id.*
[7] *Id.* at 56.

Additionally, companies embed in their design characteristics that extol trust and familiarity.[8] These actions can be deceptive. This is because the true nature of the platform may be antithetical to users' expectations of trust induced by the representations.[9] As a result, these companies stand in a strong position to undermine users' rational choice in favor of their own ends.

More importantly, notice-and-choice undermines many of the user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy. Implementing a trust-based approach to privacy law can cause many of the privacy outcomes and high-level goals sought in the Request for Comments to be realized.

Applying a privacy-as-trust regime to consumer privacy is to recognize that those who collect our data are invested with a fiduciary obligation over our information. [10] Consequently, these data collectors should be treated as fiduciaries in regard to our data.

III. Privacy-as-Trust, High-Level Goals, and Privacy Outcomes

In *Privacy as Trust,* Ari Ezra Waldman, a privacy scholar and law professor, explains that every fiduciary relationship has power asymmetry and vulnerability.[11] For example, doctors and lawyers have knowledge and skills that laymen do not possess. Consequently, a power asymmetry arises between the skilled and the laymen. As a result of this power asymmetry, laymen must rely on skilled, knowledgeable professionals to competently execute their job. In the same manner, and of similar importance, laymen rely on these professionals to maintain a higher standard of care in regard to the relationship at hand.[12]

Waldman argues that corporations that handle our data should be similarly treated.[13] This is because relationships between consumers and corporations who deal with their data contain power asymmetries and vulnerability as well.[14] Therefore, these companies should be treated as information fiduciaries. Following this logic, companies should then be held accountable for breaches in trust arising from their fiduciary relationships. Under a privacy-as-trust regime, consumer privacy law can realize many of the privacy outcomes and high-level goals sought in the Request for Comments.

First, the high-level goal of employing a risk and outcome based approach in consumer privacy law becomes possible. This is because companies would be required to act with the privacy expectations of the consumer in mind. Expectations would be guided by the content and context in which disclosures are made between consumer and company.[15] Therefore, sensitive information, for example, would be afforded a higher level of protection than other kinds of information.

This would allow companies to evaluate risk based upon the content of the information they collect as well as the context in which it is shared. Moreover, a privacy-as-trust regime

---

[8] *Id.* at 57.
[9] *Id.* at 91.
[10] *Id.* at 88.
[11] *Id.* at 86.
[12] *Id.*
[13] *Id.*
[14] *Id.* at 87.
[15] *Id.* at 86.

achieves this high-level goal without being overly prescriptive. Indeed, organizations would be granted flexibility in balancing business needs, consumer expectations, legal obligations, and potential privacy harms when making decisions about how to adopt various privacy practices. This is precisely what this high-level goal seeks to accomplish.

Additionally, privacy-as-trust is inherently a user-centric model. This is because privacy-as-trust focuses on the expectations of how certain information will be used based on trust. The user-centric outcome of maintaining that trust, is thereby accomplished. This can lead to enhanced sharing, which is good for society.[16] Additionally, this is good for companies to make a profit. This is because increased sharing would be incentivized by legitimate privacy protections. Ostensibly, this would enable companies to yield more profit by attracting and keeping more users. Illustrative of this is a recent breach of trust at Facebook, the Cambridge Analytica ordeal.[17] According to one study, Facebook lost 2.8 million users after the breach.[18] What's more, the study only accounted for the number of users that deleted their Facebook who were from the United States and under 25 years of age.[19] This illustrates the importance that trust plays in consumer-company relationships. It also demonstrates that a privacy-as-trust regime can provide mutual benefits for consumers and companies by incentivizing sharing based on trust.

Similarly, because of the flexibility afforded by the privacy-as-trust regime, the high-level goals of obtaining comprehensive application, maintaining legal clarity while maintaining the flexibility to innovate, and incentivizing privacy research would be met. This is because privacy-as-trust is not a prescriptive regime. Thus, it can be applied across various businesses and business models. Moreover, because privacy-as-trust makes clear that organizations would be considered information fiduciaries, companies are free to innovate as they wish, so long as they abide by their fiduciary duties.

Notably, innovation would not be stymied by the implementation of privacy-as-trust regime. In fact, privacy-as-trust would incentivize privacy research. Companies, seeking to abide by the privacy-as-trust regime, would want to know about the expectations of consumers in different circumstances. This would catalyze innovation to enable companies to make proper risk assessments. Additionally, it could lead to innovative solutions to privacy problems for the benefit of both companies and consumers.

In contrast, notice-and-choice does not catalyze innovation in the same way. Companies merely have to provide notice of their privacy policies and wait for users to "consent" to them.[20] This in no way incentivizes privacy research, promote user-centric outcomes, or provide companies with a risk based approach to privacy. In fact, "at least one court has held that because most of us do not read privacy policies, they cannot represent a 'meeting of the minds'

---

[16] *Id.* at 50.

[17] Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram*, VOX (May 2, 2018, 3:25 PM), https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

[18] Kurt Wagner & Rani Molla, *Facebook lost around 2.8 million U.S. users under 25 last year; 2018 won't be much better.* RECODE (Feb. 12, 2018, 6:00 AM), https://www.recode.net/2018/2/12/16998750/facebooks-teen-users-decline-instagram-snap-emarketer.

[19] *Id.*

[20] Waldman, *supra*, at 80.

and, therefore, are not valid, binding contracts..."[21] Additionally, for an average person to read all of the privacy policies applicable to them would take 76 full working days a year.[22] This poses problems for both consumers and companies, and should be replaced by a privacy-as-trust model.

IV. FTC Enforcement Compatibility

Furthermore, the high-level goal of FTC enforcement can be achieved through a privacy-as-trust regime. Although the FTC currently enforces the current notice-and-choice regime, the FTC would be strengthened by privacy-as-trust.[23] As Waldman states, "[p]rivacy-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..."[24] This would enable the FTC to regulate against corporations who use deceptive designs and practices that induce trust, and subsequently breach such trust.[25]

In fact, as Waldman points out, the FTC already has a "long track record of regulating deceptive practices that are similar to inducing trust."[26] For example, in *In re Snapchat*, the FTC went after Snapchat, an ephemeral messaging application, for allegedly misleading consumers and mishandling their data.[27] Specifically, the application's design gave users the impression that a video or picture message would disappear after a user-set duration of time expired. The time would begin after the recipient of the message opened the message. However, there turned out to be several ways in which recipients of the photographs and videos could permanently keep and utilize the media in the messages.[28] Snapchat's actions here can be fairly summed up as a breach of trust induced by the design of their platform.

Another example of induced trust by design is found in a Facebook algorithm. This particular algorithm displays friends' and family members' posts at the top of members' news feeds.[29] At first blush, this seems like a helpful design for users to see posts by people that they care about. However, it serves a hidden purpose of serving the financial interests of Facebook. This is because third-party websites and advertisements that are shared by friends and family will get priority in a given news feed. Moreover, the fact that the third-party post is presented by someone close to a Facebook user induces trust in the user.[30] However, because this design is serving a financial interest of Facebook, their interest "potentially conflicts with prevailing

---

[21] *Id.* at 18.
[22] Aleecia M. McDonald & Lorrie Faith Cranor, *The Costs of Reading Privacy Policies*, 4 I/SJ. OF L. & POLICY 540 (2008).
[23] Waldman, *supra*, at 89.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.* at 88.
[28] Complaint, *In re* Snapchat, Inc., FTC File No. 132 3078, No. C-4501 (F.T.C. May 8, 2014), https://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf.
[29] Waldman, *supra,* at 89-90.
[30] *Id.* at 90.

privacy norms and the asymmetry of power between us and Facebook."[31] This undermines the trust that was induced by the deceiving design.

In both of these examples trust was induced by companies that have asymmetrical power relationships with users, therefore making users vulnerable. In a privacy-as-trust regime these actions could be recognized as an inducement of misplaced trust under Section 5 of the FTC Act.[32] Moreover, under the FTC Act, intent to deceive need not be shown.[33] The company's conduct needs only to be shown deceptive by its likelihood to deceive.[34] Consequently, this will further incentivize privacy research and innovation. This is because companies will be galvanized to innovate products and designs that have a low likelihood of deception by keeping consumers' expectations and notions of privacy in mind.

On the other hand, it is notable that Facebook and other information fiduciaries may give our data to third parties, contingent that the third parties maintain the same fiduciary duties to users' information.[35] Thus, this would allow for companies to continue to profit in dealings with third-parties while simultaneously respecting consumers' expectations of what their data is being used for.

Waldman suggests that the FTC can regulate this type of behavior by requiring certain design changes.[36] Facebook and other organizations who use the advertisement model for revenue need not stop using the model in light of this type of enforcement. For example, by curbing the use of trust cues on advertisements, Facebook would still be able to use the advertising model, just without manipulating trust.[37] Additionally, the FTC could mandate platforms like Facebook to use designs that emphasize that an advertisement is an advertisement, and not a post by a friend.[38] Regulations such as these would "eliminate the elements that could induce misplaced trust."[39]

V. The Significance of Design and the Fallacies of an Autonomy-Based Privacy Model

The above highlights how design has the power to substantially influence consumer behavior. It also demonstrates that our deeply-held ideas of autonomy and free choice may be detrimental to our attempts at implementing an effective privacy law regime. For example, Tristan Harris, an ex-Google Design Ethicist, has explained that many apps have a similar addictive effect on users as that of slot machines.[40] The app designers do this by granting

---

[31] *Id.* at 91.
[32] *Id.* at 89.
[33] Chris Jay Hoofnagle, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY 124-5 (2016).
[34] *Id.*
[35] Waldman, *supra,* at 88.
[36] *Id.* at 92.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] Tristan Harris, *How Technology Hijacks People's Minds—from a Magician and Google's Design Ethicist* (May 19, 2016), http://www.tristanharris.com/2016/05/how-technology-hijacks-peoples-minds%e2%80%8a-%e2%80%8afrom-a-magician-and-googles-design-ethicist/.

intermittent variable rewards.[41] In other words, the apps bestow users with rewards such as a new "like" on a social media app. Consequently, the user becomes addicted to checking their phone for the "reward." What's more, these rewards are even disbursed at certain times and in certain places to exacerbate the addictive or manipulative effects that influence users.[42]

A telling study of the coercive nature of design involves an online questionnaire. The same questionnaire was embodied in two websites which required participants to give identifying information to the website before answering the questionnaire.[43] Both websites had the same exact questions.[44] Answering the questions would indicate whether the participants had engaged in risqué and sometimes illegal behavior.[45] The only difference was in the designs of the websites.[46] One website looked as if a teenager would have made it. Its font was childish-looking and it had a pixelated cartoon of a devil at the top of the page. The page was titled "How BAD are U???"[47] The other website was much more proper. Its font was formal and the page was titled "Carnegie Mellon University Survey of Student Behaviors."[48] Compared with the formal-looking website, it was found that the childish, more lighthearted website got users to admit to risqué acts of behavior over twice as many times, and illegal acts almost twice as many times, as the former.[49]

These examples speak to the power that design has on us. In fact, design is power.[50] This is not a new concept. Design has long been used to fashion power over its users. This is evident in fields from architecture to urban planning.[51] For example, it is argued that Robert Moses built low bridges in route to Jones Beach to keep the lower-class, who largely utilized the bus, from getting to the beach.[52] Perceived notions of autonomy and free choice are blurred when taking into consideration the power that design has over us.

In fact, merely using the internet requires us to share information.[53] Information is shared not only directly by users inputting credit cards to buy things or their names and emails onto social media sites, but also indirectly. Indirect information sharing is a consequence of the fact that internet browsers record "what websites we visit, what search terms we use, where we move our cursor, our IP addresses, and hardware details via ongoing behavioral tracking."[54] What all of this means is that consent cannot be valid if the alternative is not using the internet at

---

[41] *Id.*
[42] *Id.*
[43] Woodrow Hartzog, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 40-1 (2018).
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.* at 41.
[49] *Id.*
[50] *Id.* at 34.
[51] *Id.* at 34.
[52] Michael Powell, *A Tale of Two Cities,* N.Y. TIMES (May 6, 2007), https://www.nytimes.com/2007/05/06/nyregion/thecity/06hist.html.
[53] Waldman, *supra*, at 32.
[54] *Id.*

all, or if consent can be manipulated by deceptive designs. Notice-and-choice, again, fails to protect users in this manner.

VI. Learning from Fourth Amendment Jurisprudence

In many regards, consumer privacy should learn from Fourth Amendment jurisprudence. First, consumer privacy can learn how certain types and amounts of information should be categorized. In *Smith v. Maryland*, Justice Powell's dissent describes why law enforcement should only be able to access telephone numbers we dial by getting a warrant.[55] He explained that knowledge of merely one phone number we dial may not be extraordinarily revealing, however, an inventory of multiple phone numbers we dial can "reveal the most intimate details of a person's life."[56] Similarly, in *United States v. Jones*, five justices agreed that aggregated data of a person's whereabouts by way of long-term GPS tracking constitutes a Fourth Amendment search.[57]

The concept that an aggregated amount of seemingly innocuous information can lead to knowing vastly more information about a person is known as the mosaic theory of privacy in Fourth Amendment law.[58] With this in consideration, consumer privacy should treat similar amounts of information in the aggregate with more concern, regardless of what the data is. It is a patent fact that aggregated web browsing can reveal the most intimate details of a person's life; possibly even more than that of aggregated phone numbers or even long-term GPS tracking.[59] In fact, data collection of web browsing history and patterns that do not contain the name of the internet user can still allow companies to figure out exactly who the user is.[60] Therefore, similar aggregated data, even seemingly innocuous data, should be treated by consumer privacy in the same way as the mosaic theory of privacy in Fourth Amendment law.

Additionally, consumer privacy can learn a lesson in what not to do from Fourth Amendment jurisprudence. Particularly consumer privacy can learn from what Fourth Amendment law regards as the third-party doctrine. The third-party doctrine, is the rule that you have no expectation of privacy over information in the hands of a third-party.[61]

The problems with this doctrine can be illustrated by the following example. When consumers hand over information to Facebook, they in fact do have a legitimate expectation of privacy in that information. Namely, that their information will not be sold to an entity for

---

[55] Smith v. Maryland, 442 U.S. 735, 748 (1979) (Powell, J., dissenting).
[56] *Id.*
[57] Waldman, *supra*, 65.
[58] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012).
[59] Kaveh Waddel, *Your Browsing History Alone Can Give Away Your Identity*, THE ATLANTIC (Feb. 6, 2017), https://www.theatlantic.com/technology/archive/2017/02/browsing-history-identity/515763/.
[60] *Id.*
[61] Daniel J. Solove, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 102 (2011).

purposes dissonant to their expectations.[62] By abstaining from the third-party doctrine, breaches of trust will not be circumscribed by the fact that the information was no longer private. Again, companies need not refrain from selling or sharing certain information to third-parties so long as the third-party receiving the information parallels the fiduciary obligations afforded by the original parties.[63]

VII. Concluding Statement

I believe that implementing a privacy-as-trust regime will enable consumer privacy law to achieve several high-level goals and privacy outcomes sought in the request for comment. Moreover, I believe that it will be consistent with consumers' expectations of privacy while allowing companies to innovate and profit while using consumers' data. Thank you in advance for your consideration of my comment.

Sincerely,
Matthew Basilotto
J.D. Candidate
Member, International Association of Privacy Professionals
Matthew.Basilotto@law.nyls.edu

[62] Center for Technology and Democracy, *CDT Welcomes Woodrow Hartzog, Author & Professor - Privacy and Design*, YOUTUBE (May 9, 2018), https://www.youtube.com/watch?v=mksi22hFwmQ&t=1437s.
[63] Waldman, *supra,* at 88.