November 9th, 2018

Attn: Privacy RFC
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, Room 4725
NW Washington, DC 20230
United States of America

RE: Request for Comments on Developing the Administration's Approach to Consumer Privacy, Docket Number: 180821780-8780-01

Dear National Telecommunications and Information Administration:

Thank you for the opportunity to submit comments on ways to advance consumer privacy while protecting prosperity and innovation. As a law student enrolled in Information Privacy Law, this is an exciting chance to utilize classroom learning and perform meaningful research on a topic that plays an important role in modern society.

Transparency and Control

In a world where it is almost impossible to live day-to-day life without the Internet, it is critical that users have a basic understanding of what happens to their data and assurance that it is being protected. Transparency and control of data go hand-in-hand because an average user must first understand how an organization or entity collects and stores their data, then should be able to maintain some level of control over their data at various stages. The way data is stored, collected, used, and disclosed depends heavily on the privacy regime currently implemented in the U.S., known as "notice-and-choice." This system is based on privacy as autonomy and has been flagged by many scholars as highly inadequate.[1] Essentially, this regime is founded upon the notion that we, as individuals, decide when and how to disclose our data and data collectors simply provide

[1] Waldman, Ari Ezra. Privacy as Trust: Information Privacy for an Information Age (pp. 79-80). Cambridge University Press. Kindle Edition.

an opportunity to consent and an overview of their practices.[2] However, notice-and-choice is not the only regime. Privacy-as-trust is an alternative theory for data collection and treats those who collect data as "information fiduciaries."[3] Balkin's "information fiduciaries" would require experts, i.e. data collectors and processors, such as Instagram, to have power over us only when they act with the user's best interest in mind and hold them responsible when they fall short of this requirement.[4]

Understanding why the law and practices developed is key for comprehending the fundamental flaws and providing a basis for discussion on how to improve users' data privacy. Simply explained, notice-and-choice requires companies that collect user data to inform users what information they collect, how they collect it, and whom they share it with.[5] That is the notice requirement. Then, users have a "choice" to opt out or use a different platform.[6] However, it is not always that easy. There are a variety of circumstances in which a person cannot opt out and also does not truly have the option to utilize another platform. For example, many students are required to maintain accounts on websites like BlackBoard. This website is a host for professors to post readings, assignments, and grades viewable to students for classes. If BlackBoard does not offer students the opportunity to opt out of certain data collection, they are likely out of luck because it is fair to assume they may not be successful without consistent use of the website. When websites like BlackBoard properly give notice to users, they are technically on the right side of the notice-and-choice regime. The user could avoid using

---

[2] *Id.*

[3] Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U. C. Davis L. Rev. 1183 (2016).

[4] *Id.*

[5] Waldman, Ari Ezra. Privacy as Trust: Information Privacy for an Information Age (pp. 79-80). Cambridge University Press. Kindle Edition.

[6] *Id.*

the website altogether if she is uncomfortable with the policy, however it seems clear that her avoidance of the website may come at the price of her academic success. This is just one of a host of examples where notice-and-choice fails the user simply because she lacks the ability to opt out without causing her substantial harm. In modern society, it is easy to conjure up a long list of reasons why notice-and-choice is harmful to the user and beneficial to data collectors. But this is a relatively recent development that came as a consequence of the vast improvements in the technology field over the last few decades. Notice-and-choice stems from the Fair Information Practices Principles (FIPPs), which were developed from a 1973 Department of Housing, Education, and Welfare report recommending that government agencies collecting data from citizens should publicize their practice, allow individuals to correct misinformation about themselves, and ask for consent from those they aimed to collect data about.[7] The U.S. privacy protections are "sectoral" and not set by a comprehensive, overarching law. For example, the Fair Credit Reporting Act (15 U.S.C. § 1681) is applicable only to consumer reporting agencies, providers of consumer reporting information, and anyone who uses consumer reports.[8] While the U.S. does not have a nationwide privacy law, states have passed their own comprehensive laws. Specifically, California has been a pioneer in the U.S. and became the first state to enact a security breach notification law.[9] Laws like this are important because users may not be aware that their data has been compromised absent an organization informing them. The notice-and-choice regime itself does not even make mention of repercussions for security breaches, let alone informing users that their data

[7] *Id.*
[8] Jolly, Ieuan. Data Protection in the U.S.: Overview. Thompson Reuters: Practical Law. July 01, 2017. Web.
[9] *Id.*

has been compromised. In a privacy-as-trust regime, where organizations are held to a higher standard, it becomes much more clear that a breach would warrant a notification to users, or minimally, users that were affected by the breach. The current approach in the U.S. is essentially patchwork because of the sectoral nature of the laws and regulations in place. Organizations that are not required to notify users about security breaches are likely to sweep that information under the rug to avoid negative publicity. From a business perspective this makes perfect sense. However, allowing users, who are overwhelmed by privacy policies and are constantly required to share data, to be completely without a shield can be outright terrifying.

Users cannot reasonably expect to have control over their data without companies acting transparently simply because all control would be illusory. The 2017 Equifax data breach shook Americans to the core and left many wondering about their own data security. Over 140 million Americans were directly affected by this breach and learned that information from their names, addresses, social security numbers, and other sensitive data had been compromised.[10] Those affected were not supplied with many tools to safeguard their data and many deemed Equifax's response laughable. The company's response was rushed; creating PINs that corresponded to the date and time of the freeze for affected consumers, making them extremely easy to guess.[11] Further, Equifax advised people to sign up for the credit monitoring service that required users to agree to a mandatory arbitration clause.[12] Every step of the way, it became clear that Equifax was not equipped to handle this breach and that the company was scrambling. An important

---

[10] Electronic Privacy Information Center. Equifax Data Breach. November 3, 2018. Web.

[11] *Id.*

[12] Newman, Lily Hay. All the ways Equifax bungled its breach response. WIRED. September 24, 2017. Web.

takeaway from this breach for users is trying to learn as much as possible about what a company does with their data before handing it over and what types of controls they will be able to exercise in the future.

The Equifax data breach is one of many examples of situations in which sensitive data was compromised and users did not have adequate avenues of safeguarding their data post-breach. Moreover, data breaches are not the only aspect of data collection that should be concerning consumers. One famous example of a company using data in a "creepy" way is Target guessing a teen girl's pregnancy even before her father knew. [13] Essentially, a Target statistician, Andrew Pole, was able to develop an algorithm that could track major life events and market to individuals in the midst of experiencing them. There are a few brief time periods in a person's life when she is most likely to abandon her old shopping routines and stores, like Target, see this as a major opportunity to gain loyal customers. [14] Pole was able to figure out a way to determine when expecting mothers were in their second trimester and begin marketing items like diapers to them. He knew that tired parents are more likely to start buying additional items from Target while they are already in the store to purchase diapers because it saves time. Critically, this could help to create customers that are loyal to Target for years to come buying everything from diapers to groceries to clothing and so on.[15] While it may be convenient for consumers to receive ads and coupons tailored to their needs and interests, many find it flat out creepy that stores seem to know us better than our closest friends and family members. While the story of Target predicting a teen girl's pregnancy is well-known,

---

[13] Duhigg, Charles. How Companies Learn Your Secrets. The New York Times. February, 6, 2012. Web.

[14] *Id.*

[15] *Id.*

Target is far from the only company using algorithms to learn as much as possible about users. Netflix is another company that uses data to garner knowledge about its users. It is not all bad. Many people like the convenience of the algorithms Netflix uses to suggest movies and shows they may like based on past choices. However, as many Netflix users know, the reality is that the suggestions are often not on point.[16] Moreover, while the suggestions may not always be accurate, they likely improve over time as users stream more and more content.[17] Regardless of how on point Netflix's recommendations are, many people enjoy the convenience Netflix provides and it is seemingly less invasive than other services that show ads for things users have only spoken about and never searched. It turns out that a program called Alphonso can be downloaded onto users' phones when they download other select apps from the app store.[18] Interestingly, this program installs itself through other apps that users choose to download and requests microphone access that is usually not disabled when the app is not in use.[19] The purpose of this app is to provide data to TV advertisers to better target individuals who are most likely to purchase their products.[20] This is a perfect example of something that users may not know is happening and may like to have the option to opt out. Further, Alphonso may detail its privacy policy in the description used before someone downloads an app, however this may leave many people feeling at a loss. Oftentimes, Alphonso targets

---

16 Ellenberg, Jordan. What's Even Creepier Than Target Guessing You're Pregnant? Slate. June 9, 2014. Web.

17 *Id.*

18 Maheshwari, Sapna. That Game on Your Phone May Be Tracking What You're Watching on TV. The New York Times. December 28, 2017. Web.

19 *Id.*

20 *Id.*

popular children's games, such as "Teeth Fixed."[21] While there is a way to disable this feature, the fact that the use of Alphonso is so hidden by these games proves that the app developers and data collectors are avoiding transparency to collect data on the sly in a grey area that is technically not illegal. Users have control in the sense that they can disable the microphone use, however when an individual, such as a parent, does not read the privacy policy for every game their child downloads, she automatically is in a position where she is not given reasonable opportunity to opt out. This can potentially lead to a complicated contracts lawsuit hinging on the lack of mutuality, like in *Dyer*, where the company handed over customer information to NASA without informing customers.[22] The ability of companies to sneakily "listen in" on conversations without breaching any duties is why users should be given transparency and control over the data collected about them. Consumers have a right to privacy and should feel secure that data collectors are maintaining their data with the user's best interest in mind.

Harmonizing the Regulatory Landscape

The sectoral system implicated in the U.S. provides strong protections in narrow areas of the law. As a result, many states have developed their own privacy laws to fill the gaps. California is paving the way by introducing laws that require data collectors to act more responsibly with user data. From a user-centric point of view, California's laws provide for an online experience that is much more informative and transparent. However, a consequence of state laws has been a patchwork system that can be difficult for data collectors to comply with. In order to cure this defect, the U.S. must take steps to

[21] Mamiit, Aaron. Some Mobile Games Listen To What You Watch On TV: Here's How To Stop It. Tech Times. December 30. 2017. Web.

[22] *Dyer v Northwest Airlines Corps.*, 334 F Supp 2d 1196 [DND 2004].

harmonize the regulatory landscape by clarifying what organizations that process personal data must do in order to properly adhere.

The first major hurdle is ensuring that individuals are aware of their privacy rights and what protections they have based on their geographic location. The thought that a person living in California may have significantly more protections than a person living in Ohio is both frustrating and confusing for both consumers and organizations.[23] Moreover, larger organizations may decide to treat all consumers the same, meaning that they are complying at the highest standard for all, while others may choose to comply with state laws individually. Finally, this concept becomes even more challenging for organizations that process data internationally due to laws like General Data Protection Regulation (GDPR) that dictates the privacy standard in the European Union.[24]

As previously mentioned, the reason that privacy laws are crafted in such different ways is because of the way privacy is thought about at a fundamental level. Generally, privacy is not considered a basic right in the U.S., whereas in the EU it is considered a basic tenet.[25] In the U.S., the right to privacy is alluded to in the fourth amendment.[26] California, however, has taken a different approach and specifically included privacy as a fundamental right.[27]

California's inclusion of privacy as a basic human right has led to the development of laws that go above and beyond to protect its citizens' right of privacy. In

---

[23] Privacy Protections in State Constitutions. National Conference of State Legislatures. November 7, 2018. Web.

[24] 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 L 119, 4.5.2016, p. 1–88.

[25] *Id.* at Ch. 1, Art. I.

[26] U.S. Const. amend. IX.

[27] Cal. Const. Art. 1, § 1.

2004 and amended in 2013, California became the first state to require commercial websites and online services to post privacy policies with California Online Privacy Protection Act (CalOPPA).[28] This law applies to any person or company collecting personally identifiable information (PII) on Californians online.[29] This law requires data collectors to meet a list of requirements that are meant to increase transparency and control for consumers. For example, a website must disclose whether a third party can collect PII from users that visit their website.[30] This type of disclosure seems especially critical after the Facebook-Cambridge Analytica scandal where Cambridge acquired private data from Facebook for tens of millions of users without their knowledge, leading to a number of class action lawsuits.[31, 32] In many circumstances, companies may try to cover these breaches up to avoid negative press attention. Unfortunately, laws like CalOPPA are sometimes the only reason users are informed that their data was compromised. Despite the law applying only to California citizens, companies often become accountable to all users affected by a breach because news travels quickly in the modern age of the Internet. In some cases, the backlash may actually not be as tragic for a company that is upfront with users because people tend to respect honesty.

The U.S. is at a crossroads when it comes to improving privacy outcomes. Much of the world considers the U.S. behind the times, especially after the passage of GDPR, because there is no federal law protecting citizens' privacy online. In addition, as the

---

[28] Consumer Federation of California. California Online Privacy Protection Act (CalOPPA). Education Foundation. July 29, 2015. Web.

[29] *Id.*

[30] *Id.*

[31] Confessore, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. The New York Times. April 4, 2018. Web.

[32] *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 2018 US Dist LEXIS 101061 [JPML June 6, 2018, No. MDL No. 2843].

number of states passing their own versions of online privacy law increases, the more challenging it becomes for organizations that collect and process data to properly comply. As it stands, the U.S. already has a variety of departments overseeing the sectoral laws. These departments have focused goals and strive to protect consumers in a variety of areas, such as medical information (HIPAA) and unfair trade practices (FTC Act).[33, 34] However, the lack of an overarching federal law and the mosaic of state laws that have been enacted have led to an American landscape that is essentially a tangled web of contradictory laws. American consumers deserve to know their privacy rights and must understand their protections in order to be diligent consumers. Further, data collectors and processors need a structure that is feasible to adhere to that way they can maintain their businesses in a safe and effective way. This starts with the harmonization of the regulatory landscape free from patchwork laws and, instead, an environment that allows for a symbiotic relationship between organizations and consumers.

Thank you for this opportunity to participate in this call for comments. Your time and consideration is greatly appreciated.

Sincerely,

LeeAnn Monteverde

[33] U.S. Department of Health and Human Services. HIPAA Enforcement. Health Information Privacy. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html. Web.
[34] Federal Trade Commission. Protecting America's Consumers. https://www.ftc.gov/. Web.