PUBLIC DOCUMENT

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

Re: Docket No. 180821780– 8780–01
Developing the Administration's Approach to Consumer Privacy

To Whom It May Concern:

My name is Merisa Horgan and I am writing on behalf of New York Law School's Information Privacy class to comment on, "Developing the Administrations Approach to Consumer Privacy". The purpose of this comment is to emphasize the need for privacy-trust based approaches in the transparency and clarity of user-centric privacy models, the harmonization of privacy laws utilizing the California Law, and the implementation of privacy by design in order to ensure the safety of our consumer data while still allowing for innovative development. It is imperative that we adjust our current privacy models so that we can better protect our consumer data and allow our privacy safety to evolve as our technology does.

I. Transparency

Every day that we go online, download a new app, or order a new item from amazon, we are sharing our information with an online platform. We provide our telephone numbers, our credit card information, or addresses and various other forms of personally identifiable information with the somewhat naïve idea that our information is

being protected by the companies we engage with. It is almost impossible to live in the modern world without having some sort of online presence, and it is even harder to have an online present without releasing personal information. Yet, although we trust these companies and online platforms with some of our most vital information, trust is not currently a key component in our privacy laws.

Currently, the Federal Trade Commission requires online commercial companies to give "Notice and Choice", which includes a description of what when and how they use the data they collect and provides users with an option to opt out of the contract. This is normally displayed as a privacy policy on websites, and is proven to be ineffective. Most people don't read the privacy policy statements that are given on websites, and even if they do, it is rare that someone will opt out because they will lose most benefits of the website. For example, in Amazon's privacy notice in March 2014, it states under the 'Information You Give Us' section that, " We receive and store any information you enter on our Web site or give us in any other way. You can choose not to provide certain information, *but then you might not be able to take advantage of many of our features."* [1]. It then goes on to repeat this same statement in other sections, making opting out seem less desirable. Although this provides consumers with a way to opt out of data collection, it also puts them at a disadvantage if they do so, and gives a significant amount of power to Amazon.

Ari Ezra Waldman describes a different approach to privacy in his book, "Privacy As Trust". He explains that rather than privacy being viewed in an autonomous manner,

[1] McGeveran, Willam. *Privacy and Data Protection Law* (pp 168). Foundation Press, 2016.

it should be viewed as trust, and companies like Google, Amazon, and Target should be considered 'Information Fiduciaries'. Waldman states that, "Rather than limiting corporate responsibility to giving us a list of data use practices for rational privacy decision-making, privacy-as-trust recognizes that data collectors are being entrusted with our information. Therefore, they should be held to a higher standard than mere notice. They are, in fact, fiduciaries with respect to our data, and should be obligated to act in a trustworthy manner." [2]This infers that because these companies have so much of our data, rather than only giving us the option to opt out of whatever privacy policy they choose to adhere to, it requires them to adhere to certain standards that require trustworthiness. It puts the ball in the companies court, rather than making it up to the user whether they wish to participate or not – with seemingly no option not to.

Take again the Amazon example displayed above. There are many benefits to giving your information to Amazon. The list includes: shopping customization, requests, improving store quality and communication. These are great benefits that most people generally like having. It is very convenient to go onto Amazon Fresh and have a set list of groceries from your previous purchase so that you don't have search for eggs again. But, if the only option you have when it comes to your privacy and control of information is to entirely opt out, it is unfair to the consumer and puts them at a huge disadvantage. Rather, it should be up to the company to be responsible with your information and create that center of trust, where although you are giving over information, you know that they are required to handle it properly and with consequence.

---

[2] Waldman, Ari Ezra. *Privacy as Trust: Information Privacy for an Information Age* (pp 85). Cambridge University Press. 2018.

Waldman then goes further to explain how vulnerable we are to these companies. He states, " They know everything about us; trade secrecy keeps their algorithms hidden from us. They monitor every step we take online; we know little about how they process our information. "[3]This evidences the huge gap in transparency that exists between consumers and the companies tracking and disseminating their data. Because we cannot know what the companies are doing with our data based on trade secrets, algorithms and various company processes, we are at their mercy. Trust is gone when we do not know what is happening with our information, and suddenly it is being marketed to third parties, breached, or sold without consent. Waldman again furthers this notion by stating, "We share information with others including online data collectors, with the expectation that those companies will treat our data according to prevailing norms and promises. We experience the further sale or dissemination of our data to unknown third parties as violations of our privacy precisely because such dissemination breaches the trust that allowed us to share in the first place. " [4] We hand over our information because we have an innate trust in these companies. When we find out our information is being distributed without our knowledge due to a lack of transparency between consumer and company, the trust is gone.

In order to best attack this transparency problem, the way privacy is viewed must change. Companies should be held as Information Fiduciaries who are meant to protect and guard our information, so that even though we are still providing them with information, the way they are required to hand it is much different.

---

[3] Waldman, Ari Ezra. *Privacy as Trust: Information Privacy for an Information Age* (pp 86). Cambridge University Press, 2018.

[4] Waldman, Ari Ezra. *Privacy as Trust: Information Privacy for an Information Age* (pp 87). Cambridge University Press, 2018.

II. Harmonization

The second issue with current privacy law is the complete lack of harmonization between the states. Various states have various laws on privacy making it difficult to have a set privacy standard for companies to follow. Additionally, many privacy laws are only geared towards a specific industry or practice, such as the Children's Online Privacy Protection Act, or the Health Information Portability and Accountability Act (HIPPA). These privacy standards were initiated because of the sensitivity of information being shared and have a set a precedent for forthcoming privacy law. Because of the lack of consistency between state and industry, it is hard to innovate privacy standards, and it is difficult to maintain privacy needs for consumers and companies alike.

In June of 2018, the California Consumer Privacy Act was voted into law. This California law is huge change to consumer privacy and is a wonderful demonstration of what could and can be implemented across the United States. The Act is founded on three principles including: transparency, control and accountability, in which it allows consumers to understand what is happening with their information, and also own their information. Due to the enactment of this law, Californians are now able to: know all data collected by a business on you (twice a year, free of charge), right to say no to sale of information, right to delete data which you have posted, the right to sue companies for select reasons, the right not to be discriminated against based on collected data, right to be informed of what categories are being collected on you, mandated opt- in for sale of children's information, right to know categories of third party information shared, right to know categories of sources of information of whom your information is acquired, and the

right to know the business or commercial purpose of collecting your information. [5]This law is heavily focused on consumer protection and allowing the consumer to know exactly what is going on with their data.

The great benefit of conforming to an act like this countrywide, is the amount of trust it will instill between companies and consumers. In the transparency section, the idea of Information Fiduciary was discussed and the importance of the privacy-as-trust principle, as opposed to privacy as autonomy. This act is a direct reflection of privacy-as trust. By creating such a dynamic law that encompasses everything a consumer should know about their data and where it is going, allows for a greater relationship between company and consumer. It will provide the consumer with the aggregate knowledge that allows them to entrust their information with companies and in turn companies can grow and develop they way they need to.

It will also help the hindrance of company's ability to travel state lines. Because there is such a difference between states privacy laws, companies are hindered and confused what protocol to follow. If Colorado requires disclosure, while Idaho doesn't, it becomes difficult to maintain consistency in products and sharing information. This also puts a great strain on innovation. It is difficult to develop products and share them if there are such varying levels of privacy law throughout the United States. You need a standard line of trust that people can rely on in order to ensure that they trust in companies development and new products and they continue to participate in the economic environment.

[5] California Consumer Privacy Act. California. https://www.caprivacy.org., 2018.

By harmonizing the laws of the states to better conform to a similar act as the California Statute, would benefit everyone involved. Consumers would understand what is going on with their information and be more apt to share it. Companies would be more responsible with sharing their information and providing more care to their consumers. Innovation would progress because there would be a line of trust between company and consumer. Without that, there is a complete disconnect between companies.

III. Privacy By Design

Another key aspect in the development of privacy protection is implementing Privacy by design. In order for companies to keep up with privacy demands, and for privacy to evolve with technology, it must be involved at the very beginning stages of development.

In May of 2018, the European Union enacted what is known as the General Data Protection Regulation (GDPR). It is the most robust call on data privacy to date and is an extensive regulation that is maintained across the European Union and also extends to any foreign countries or companies that plan to do business in the European Union. Included in the GDPR is Article 25: Data protection by design and default, and states as follows:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and

organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article. [6]

What this specific article essentially does is requires companies to include privacy at the very beginning stages of design. It requires that a controller will implement data privacy processes when the process is starting and as it develops along the way.

The importance of this article and, what is shows the world, is that privacy needs to be considered long before it becomes a problem. With the way that technology is developing it is hard to keep up with privacy policy and technology at the same time. Algorithms determine so much of what we see online, and who we date, and sooner than later robots will not be so far off. In order to manage that, privacy has to be included at

[6] General Data Protection Regulation. Art. 25. https://gdpr-info.eu/art-25-gdpr/. ,2018.

the forefront. It should be maintained by engineers that build the programs so that when a program is designed it, already has the safeguards in place to prevent privacy disasters.

An example of privacy by design is something like a dating site. If a dating site is developed you would assume that during its development, the privacy of the people involved and the sensitivity of the information they would be sharing would be considered. If someone goes onto a dating site and reveals personal information about themselves, they assume some trust in that company and that it will be kept secret. There are many personal things that go into dating. When an app, much like Hinge, Bumble, or Tinder is used there should be privacy settings built into the design so that those people are protected.

In Woodrow Hartzog's , "Privacy's Blueprint" , he describes a similar situation that happened on Facebook. He detailed a young woman who was a lesbian but had not come out to her parents yet and did not want them to know. Because Facebook had not designed its discussion groups with privacy settings, the young woman was added to a group called "Queer Chorus" and it was publicly displayed as a note to friends at which her Father became aware. [7]

This is incredibly personal information. It is information that this young girl most certainly did not want to be publicly displayed on a social media platform that she trusted. Because Facebook failed to include privacy settings when it was developing its discussion platform, there was not way for this girl to control what information was getting out. She couldn't make the choice to reveal that information on her own- Facebook did so for her.

[7] Hartzog, Woodrow. *Privacy's Blueprint* (pp 1). Harvard University Press, 2018.

If privacy is not considered at the beginning stages of design, many things can go wrong. Information such as this young girls can be release without her knowledge, people can lose social security numbers, credit card information and so much more can be revealed at the drop of a hat, just because companies failed to get involved early enough.

In order for privacy to be protected entirely, it must be taken seriously, and it must be considered at early stages. The United States should look towards the GDPR for guidance and recognize that in order to safeguard our security as the future evolves, we must begin the process at developmental stages in technology and research should be done.

Conclusion

In order for privacy to advance with the modern age, changes need to be made to ensure that consumer data is protected as technology evolves. First, there needs to be transparency in the ways in which our consumer data is used. This will be achieved by approaching privacy issues in the lens of privacy by trust and not by autonomy. Information Fiduciaries should be acknowledged, and a trust should be built between consumer and company. Second, harmonization of laws must happen between the states. The California Consumer Protection Act is a great example of what can be done in the United States and should be used across the board. And third, Privacy by design should be implemented in the early stages of developing technology. In order to ensure our safety it must be considered early on. By committing to all of these modifications, the privacy of Americans is much better suited and innovation will thrive.

Very Respectfully,