Comments for Docket No. 180821780–

8780–01

To Whom It May Concern:

Consumer privacy was not seen as being a pressing issue amongst Americans prior to the evolution of technology. As society has developed becoming obsessed with the ever-changing technology and worried about the problems arising from that technology, Americans have become concerned with the protection of their personally identifiable information. Consumers are concerned about keeping their information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.[1] As a second-year law student with an interest in information privacy, I was excited to learn that the National Telecommunications and Information Administration was seeking comments on ways to advance consumer privacy. After reviewing the broad outline for the direction that Federal action should take, it is apparent four things are missing. Below I will explain what is missing and how the administration would need to go about to implement what is missing is. I will then proceed to explain why I think what is missing is needed and touch on any potential pushback that may come about.

The first thing missing is the concept of privacy by design. Privacy by design occurs when a company designs their products that contain consumer data to emphasize keeping the data protected.[2] Individuals designing these products must design it in a way that protects such

[1] U.S. General Services Commission, Rules and Policies - Protecting PII - Privacy Act, (October 31, 2014), https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.
[2] Woodrow Hartzog, Privacy's Blueprint The Battle to Control the Design of New Technologies, 15-6 (2018).

information to the greatest abilities available.[3] The companies that the developers work for must also change their business models to shift more of a focus towards protecting this information.[4] On paper this concept seems quite simple and easy for companies to implement; however, in practice many questions as to how it operates.

For the administration to incorporate privacy by design into their approach, the administration must understand and find a way to implement Ann Cavoukian's 7 Foundational Principals of Privacy by Design. Through understanding, and eventually implementing, those principles, the administration will be able to incorporate privacy by design. Cavoukian says that for a company to comply with the principle of privacy by design they must incorporate the following: proactive not reactive; privacy as the default; privacy embedded into design; full functionality; end-to-end security; visibility and transparency; and respect for user policy.[5] By themselves, Ann Cavoukian's 7 principles of privacy by design are just empty words. Even with the explanations she provides, there is no guidance or direction for companies to apply these principals.

The reason that the administration should implement these principals into their approach is that it will create trust between the consumer and the company. Trust is essential in the field of privacy.[6] Consumers that believe companies are doing everything they can from the beginning of the process to protect consumer data will be more willing to share information with these companies.[7] Without this trust, consumers will be reluctant to share data, which in turn, hurts the company more than the consumer. Gaining this trust will also limit the impact on companies if

[3] Id.
[4] Id.
[5] Ann Cavoukian, Privacy by Design The 7 Foundational Principles, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.
[6] Ari Ezra Waldman, Privacy as Trust Information Privacy for an Information Age 49 (2018).
[7] Id at 105.

there is a breach of consumer data. Consumers will know that the company did all they could to protect the data and are going to take great measures to fix the issue. This will allow the consumer to feel comfortable using this product again. Without trust, consumers may resort to alternate companies that offer the same products or services.[8] To implement privacy by design Cavoukian's seven foundational principals must go from being principals to being functional.

A second thing missing is a system of punishment for violators of current or future privacy laws. The seventh high-level goal of the administration is to continue to have the FTC to act as the enforcement board; however, in that goal, there is nothing suggesting what the FTC can and cannot do if privacy laws are violated.[9] Under current policies and procedures, the FTC issues consent decrees that are settlements between the parties where there is neither the admission of guilt or liability.[10] No punishments are handed down in the decree. The only punishments that will come are if the companies are found in violation after the decree.[11]

To implement this new system, the FTC should be able to hand out punishment in the form of monetary fines. The administration can attempt to follow suit on what the GDPR has implemented as their form of punishment. The GDPR imposes a fine on companies that are found to be in violation of multiple provisions of the GDPR.[12] Section 83.3 states that the firm will be fined according to the most serious violation, in comparison to being penalized for each separate infraction.[13]

---

[8] Id at 49.
[9] David J. Redl, Developing the Administration's Approach to Consumer Privacy, Fed. Reg., 48600, 48603, September 21, 2018.
[10] Federal Trade Commission, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
[11] Id.
[12] GDPR Online Resources, Fines and Penalties, https://www.gdpreu.org/compliance/fines-and-penalties/.
[13] Id.

If the firm is found to be violating the provisions contained in Articles 8, 11, 25-39, 42, 41(4) and 43 the fine is the higher of an amount up to ten million Euros or two percent of the company's annual revenue of the prior fiscal year.[14] A stricter fine is imposed if the firm is found to be violating the provisions contained in Articles 5, 6, 7, 9, 12 - 22, 44-49, Chapter IX, or any non-compliance with an order by a supervisory authority.[15] A firm that is found violation several of these provisions is subject to a fine of up to twenty million Euros or four percent of the worldwide revenue of the prior fiscal year, whichever amount is higher.[16] Through imposing a fine system such as this, it is clear that the European Union takes consumer privacy seriously. Also demonstrating that companies are going to be held liable for their actions, regardless of the size or popularity of the company.

A similar system of punishment should be included into the current plan because companies will be held liable if they are not in compliance with privacy laws. Under the current FTC system, companies only need to do the bare minimum to protect consumer data knowing there is little that the FTC will and can do. A fine system such as the one explained above will not allow companies to do this. It will now be a motivating force for companies to change their policies and procedures to focus on protecting consumer data to prevent the company from facing such crippling fines. A fine system is yet another way that the principals of privacy by design can be implemented. Facing fines can cause companies to account for the privacy laws to be considered and implemented at the time of design and creation rather than after a breach or leak has occurred. Companies will no longer be able to sit back and wait for a problem to arise before they consider consumer data privacy.

---

[14] Id.
[15] Id.
[16] Id.

Through incorporating this change, the administration will receive pushback from companies now having to change their business model or platform. The majority of the pushback will come from small to midsize companies.[17] Imposing a fine of such magnitude has the possibility of ending small to midsize businesses.[18] These companies do not have the same resources and ability to hire date protection officers that large companies can.[19] The world's largests companies, such as Google and Facebook, are spending tens of millions of dollars to prepare for the changes that come with the GDPR.[20] Companies here in the United States would be willing to do the same if a similar fine system was implemented.

Similarly, the budgets of these businesses are not prepared for the changes needed to now comply to avoid fines.[21] To be prepared companies are going to have to take money from other places in the budget, which could still lead to fines or a collapsing business.[22] For example, Uber Entertainment, an online gaming company, is going to shut down because it will cost them too much to rewrite the game or migrate it onto a different platform to comply with the GDPR.[23] The chief technology officer at DivvyCloud, Chris DeRamus, stated that smaller companies "don't have the apparatus and the team in place to actually really continuously support this kind of compliance."[24] The only pushback that would come from large companies would be that these

[17] Justin Dolly, How GDPR Will Affect Small and Midsized Businesses, (May 29, 2018, 12:10 PM), https://www.csoonline.com/article/3276336/small-business/how-gdpr-will-affect-small-and-midsized-businesses.html
[18] Id.
[19] Id.
[20] Ivana Kottasova, These Companies are Getting Killed by GDPR, (May 11, 2018, 6:39 AM), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.
[21] I-Scoop, How the GDPR Impacts and Suffocates Small and Medium Businesses, https://www.i-scoop.eu/gdpr/gdpr-small-medium-businesses/.
[22] Id.
[23] Kottasova, Supra.
[24] Id.

problems would now fall on those in the C-suite.[25] However, due to the millions of dollars and vast legal teams, these companies are well suited to handle any pressure on these individuals.[26]

For the administration to combat this potential pushback, a fine system identical to that of the GDPR should not be implemented. Doing so would directly prohibit the administration from achieving one of their eighth goal. This goal calls for the federal action taken should not have a large impact on small businesses that do not collect, store, or maintain a great deal of consumer data.[27] A fine system like the GDPR's does not care if the organization is small or large if you are in violation you are fined. That is why the administration must develop a fine system having lesser of an impact on small businesses. What that fine system ultimately looks like and functions is for the administration to decide. The FTC needs to have a system of fines available at their disposal.

A third thing missing from the administration's plan is a cause of action for victims of a data breach whose information has not been used but only accessed. Individuals whose data was not used are unlikely to recover under any applicable law because courts do not think that harm was done. Unless their data has been used in a way that causes harm, the individual whose data is now in the hands of unauthorized person(s) or entities must go on about their life as nothing happened. Is there no harm done to the individual whose data, that is capable of altering someone's life, is now in the wrong hands? For example, take the recent Equifax breach where an estimated 145.5 million people were impacted.[28] Not all of those 145.5 million people had

[25] Forbes Technology Council, 15 Unexpected Consequences of GDPR, (August 15, 2018, 9:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#36ee298694ad.
[26] Id.
[27] Redl, supra.
[28] CBS/AP, Equifax Data Breach Affected Millions More Than First Thought, (October 2, 2017, 5:55 PM), https://www.cbsnews.com/news/equifax-data-breach-millions-more-affected/.

their data used in a way to hurt them but their data was compromised and has the potential to be used.[29]

Under current privacy law, those individuals would be unlikely to recover. It is not right that millions of individuals are unable to recover for the failures of companies, such as Equifax. Millions of people are now living in fear because their data was compromised and still is vulnerable to being used. Yet we do not allow them to recover, and only those whose data was used can recover. That is why a law must be created providing for a cause of action to allow for individuals whose data was accessed unlawfully to bring suit against the company who is responsible for preventing such access.

The reason that the administration must allow for such suits is that it is a method of accountability. Companies will potentially face lawsuits from all of the victims of a data breach along with potential fines that may be imposed. This would provide companies with the incentive to adhere to the principle of privacy by design. For these companies to avoid facing these lawsuits, as Equifax would face 145.5 potential suits, companies would need to create their product or service encapsulated with the highest security measures. Allowing for these new victims of data breaches to sue is not forcing companies to implement privacy by design. There is no fine for not doing so. It would be in their best interest to avoid a multitude of lawsuits by devoting time and resources at the outset to try and prevent this.

It is clear that such suits will generate great pushback from companies arguing that data breaches are inevitable.[30] There is no doubt that a data breach will eventually occur even if a company installs the latest and greatest security protocols.[31] That is why if a company is able to

[29] Id.
[30] Security Magazine, Are Data Breaches Unavoidable, (October 29, 2018), https://www.securitymagazine.com/articles/89523-are-data-breaches-unavoidable.
[31] Id.

demonstrate that their product was created with the best security measure and that they continuously updated that security, then the damages a victim will be limited. That is not to say that a company is completely free from liability by demonstrating this. This provision is a way to protect companies from being bankrupted when they did everything they could. Having such a provision will allow the administration to achieve their goal of protecting small businesses that do not collect much data.[32] These smaller companies would not be forced to close simply because of a breach. These companies would just have to spend the time and resources to meet this criterion.

A fourth thing that is missing from the plan is a more direct notice and consent system. The notice and consent system notify users the way in which companies collect, use, and store data the notice portion operates by companies telling users about the collection, usage, and storage in a privacy policy.[33] These policies contain many legalese, are astronomically long, and are often hidden company's websites and applications.[34]

The consent portion operates by the user of the site or product consents to whatever is contained in the privacy policy.[35] If the user does not want to consent then the user is free to choose another site or product.[36] Complications relating to the consent portion arise when there is no alternative for the user. For example, if I do not like Facebook's privacy policy implications I do not have to use Facebook and can use another social media site. The problem is that there is no true alternative site with a similar platform to Facebook. Leading me as a user to have no option but to use Facebook or have no social media.

---

[32] Redl, supra.
[33] Robert Sloan & Richard Warner, Beyond Notice and Choice: Privacy, Norms, and Consent, SSRN Electronic Journal 370 (2013).
[34] Id.
[35] Id.
[36] Id at 370-1.

A more upfront system would immediately notify the user the way in which their data is going to be collected, stored, and used. This is known as an opt-in pop-up.[37] This new system would also give users the opportunity to give actual consent.[38] The creator of the product can provide a direct link to the privacy policy as well as specifically telling the user what data may be analyzed.[39] For example, I recently opened a weather app on my phone and before seeing the weather for the day, I was presented with an opt-in pop-up. This pop-up told me that the company or its third-parties would analyze my IP Address, AD ID, and LAT/LONG. I was provided with the option to change my data settings, to agree to this, or to decline. After making my selection I am then able to use the app as normal. This is the type of system the administration should require companies to provide for the first time a user uses a product.

The reason that the administration should implement this is that it provides users with a clear notice on what is potentially going to occur to their data. Users are also given the ability to consent by physically clicking or touching to agree. This new system would accurately be a notice and consent system. It should also be implemented because it is now something companies that conduct business in Europe have to implement under the GDPR. Recital 32 of the GDPR no longer allows for consent to be given by the user continuing to use the site.[40] Adopting this new system would allow the administration to achieve their goal of interoperability.[41] The United States and the European Union would both require companies interacting with their consumers to require this opt-in pop-up.

---

[37] Wisepops, Popups and GDPR: What You Need to Know, (May 21, 2018) https://wisepops.com/email-popups-gdpr/.
[38] Id.
[39] Id.
[40] Wisepop, supra.
[41] Redl, supra.

The only pushback that would come because of this new requirement is that companies would be unwilling to spend the time and resources developing such a system. The only way this is a valid argument is if these companies do not operate in Europe. Those non-European companies would have to spend the time and resources developing this software. However, for the companies that do operate in Europe, this technology is going to be mandatory by 2020. Therefore, all these companies would need to do is to implement it into their U.S. based products. As for the companies not operating in Europe, yes there would be time and resources spent but it would be beneficial to the users. There would be more openness to the users and the users would trust the company more.[42] With that trust comes the user likely sharing more information with the company.[43] In conclusion, this devotion of time and resources will allow still allow the company to get consumer data while still allowing users to feel comfortable with sharing their data.

In conclusion, the administration, through their high-level goals, set out a great start to the advancing consumer privacy law. However, as I have set out above, there are four things missing from the plan. Without the implementation of privacy by design, a form of punishment, a new cause of action for those whose data is not used, and an update to the notice and choice system, the administration will not achieve their entire goal of advancing consumer data privacy. These concepts are needed in any consumer privacy law that is enacted and without them consumer privacy laws will remain the same. There will be little to no protection of consumer data. Change is needed in the area of consumer privacy and an effective change can be achieved with the inclusion of these four things.

[42] Waldman at 58.
[43] Id.

Sincerely,

Zachary Richards