November 9, 2018

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

Via email: iipp2018@ntia.doc.gov

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

As a third year law student at New York Law school I recognize how my education has engrained in me, a deep appreciation for the law. I am continuously fascinated by how the law transfigures in response to society's ever-changing landscape. In a time where technology is advancing at a rapid pace, it is crucial that the law evolve as to tailor to innovative developments that have become an integral part of our everyday lives.

I graciously welcome this opportunity to write to the Department of Commerce and contribute to the National Telecommunications and Information Administration's (NTIA) proposal on ways to advance consumer privacy while protecting prosperity and innovation. I respectfully submit these comments in the hopes that my words can offer guidance on how some of the set fourth privacy goals and outcomes can be achieved. In addition to offering clarity to this systematic approach, I hope to pinpoint specific risks that may arise while navigating through the complexities of privacy related issues.

The following comments will primarily discuss why it is imperative that the NTIA recognize privacy harm as an actual "harm" when implementing a voluntary risk-based Privacy Framework. Second, it will address harmonization and issues that may arise as a result of implementing a harmonized privacy policy.

I. Recognizing Privacy Harm as a Harm

The NTIA should recognize "privacy harm" as a harm in its approach to create a voluntary risk-based Privacy Framework. More specifically, these comments recommend that the NTIA generally characterize the types of privacy harm that exist as to enhance our understanding and approach to these harms.[1] The NTIA's privacy framework should be strategically based on the types of privacy harms it hopes to protect consumers from. It is apparent that risk-based flexibility is at the heart of the Administration's approach. With this in mind, the NTIA should acknowledge the privacy harms they don't want to risk.

Although, lawmakers and courts recognize the harm of breaches, the definition of "privacy harm" should be expanded as to clarify what exactly constitutes privacy harm.[2] It is crucial that we develop a legal approach when identifying what qualifies as privacy harm because in doing so, "the limits of privacy law will be set, thus determining the scope of innovation in high tech."[3] Furthermore, the "U.S. legal framework should recognize and provide mechanisms to address the harms that result from privacy violations."[4] As the NTIA points out, every day people interact with a variety of technological products and services as an essential part of their daily routine. With an increase of users comes an increase in the potential for privacy harm. However, absent a legal principle that captures various privacy related claims it is difficult to "grasp the scope of risks at issue" and implement a fully effective legislative framework.[5]

---

[1] Privacy and Data Security Harms, CONCURRING OPINIONS, https://concurringopinions.com/archives/2014/08/privacy-and-data-security-harms.html (last visited Nov 3, 2018).
[2] What Exactly Constitutes a Privacy Harm?, AAF, https://www.americanactionforum.org/insight/exactly-constitutes-privacy-harm/ (last visited Oct 23, 2018).
[3] *Id.*
[4] *Id.*
[5] David J. Baldwin, Jennifer Penberthy Buckley & D. Ryan Slaugh, *Insuring Against Privacy Claims Following A Data Breach*, 122 INSURING AGAINST PRIVACY CLAIMS FOLLOWING A DATA BREACH.

It is apparent that "the problem of defining harm is one of the most important in privacy law."[6] This issue remains prevalent today as can be seen in a number of cases. For example, in 2016, the Supreme Court's ruling in *Spokeo v. Robbins* brought the fundamental question of privacy regulation to the surface.[7] Here, Thomas Robbins brought suit against Spokeo, a company that conglomerates data on people based on online and offline sources. Robbins claimed that Spokeo violated the Fair Credit Reporting Act (FCRA) when they included inaccurate information in his online profile. Robins claimed that these false characteristics portrayed on the profile harmed him in that the company's portrayal of him hindered his ability to get a job.

After being tried in the district court, this case was dismissed. The court held that Robbins could not show any actual harm. Therefore, the court determined that he did not have standing. In response to this decision, Robbins appealed by filing a no-injury class action suit. He claimed that the harm that he suffered came not from a particular injury, but from the fact that Spokeo violated the FCRA statute. [8] Eventually this case made its way up to the Supreme Court. In 2016, the highest court determined, that "Robbins needs to have an "injury in fact" that is both "concrete and particularized."[9] Furthermore, the Supreme Court determined that in order to bring a class action suit, even if there is a statutory violation there has to be a concrete injury. The Court pointed out that a concrete injury is not necessarily a tangible injury.[10] However, the Supreme Court "didn't go so far as to define the boundaries of these concrete, yet intangible, harms."[11]

---

[6] Developing the Administration's Approach to Consumer Privacy, FEDERAL REGISTER (2018), https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy (last visited Nov 6, 2018).
[7] *See* What Exactly Constitutes a Privacy Harm?, AAF, https://www.americanactionforum.org/insight/exactly-constitutes-privacy-harm/ (last visited Oct 23, 2018).
[8] *Id*.; Spokeo v. Robins, 136 S.Ct. 1540 (2016).
[9] *See* What Exactly Constitutes a Privacy Harm?, AAF, https://www.americanactionforum.org/insight/exactly-constitutes-privacy-harm/ (last visited Oct 23, 2018).
[10] *Spokeo v. Robins*, 136 S.Ct. 1540
[11] *See* What Exactly Constitutes a Privacy Harm?, AAF, https://www.americanactionforum.org/insight/exactly-constitutes-privacy-harm/ (last visited Oct 23, 2018).

The *Spokeo v. Robbins* case serves as an example as to why the NTIA should work towards recognizing privacy as a harm, specifically what violation of privacy qualifies as a privacy harm or injury under the law. The mere fact that this type of ambiguity exists in privacy law is extremely problematic. It fosters obscurity in our legal system, making it difficult for organizations to know when they have harmed an individual's privacy thereby producing an injury. Such ambiguity also creates confusion for the individual. It makes it difficult for an individual to know when they have been harmed in the eyes of the law such that they have standing to bring suit and recover for their injuries. Here, even though Spokeo's violation arguably caused Robbins to suffer an injury, the ambiguity of privacy harm prevented Robbins from having standing to recover.[12]

Another case that demonstrates the importance of defining harm in privacy law can be seen in *Curry v. AvMed*. In 2009 two company laptops were stolen from a health insurer's corporate offices.[13] The laptops were sold to a dealer in stolen property and contained unencrypted personal information of 1.2 million insurance customers.[14] This unencrypted information included the customers' names, contact information, Social Security numbers and sensitive medical data. Similar to the Court in *Spokeo*, the district court initially dismissed the case for failure to state a cognizable injury.[15]

However, the litigation deviated from the standard course when the 11th Circuit reversed the district court's ruling in September 2012. The 11th Circuit determined that "a claim of actual identity theft arising from a data breach causing monetary loss" qualifies as a sufficient injury for

[12] *Spokeo*, 136 S.Ct. at 1549.
[13] *See* The Privacy Advisor | The Evolving Nature of Consumer Privacy Harm Related reading: Podcast: A discussion with FTC Commissioner Rohit Chopra, INSIDE THE EPRIVACY REGULATION'S FURIOUS LOBBYING WAR, https://iapp.org/news/a/the-evolving-nature-of-consumer-privacy-harm/ (last visited Nov 1, 2018).Consumer-privacy (last visited Nov 6, 2018).
[14] *Id.*
[15] *Id.*

standing purposes.[16] Additionally, the circuit court approved potential recovery for class members who did not experience theft but paid premiums that were intended to contribute to the costs of adequate data security.[17] In other words, privacy harm or injury was recognized by the court in *AvMed* without the consumers needing to show "direct financial losses."[18] The court approved a "$3 million class-action settlement to compensate victims of a data breach *without* a claim for realized financial harm."[19] This case reflects the "evolution in the notion of consumer privacy "harm" that is taking place in the courts and through the Federal Trade Commission."[20]

Both the *Spokeo* and the *AvMed* case show how courts "continue to grapple with the definition of consumer privacy harm on a case-by case basis."[21] Courts notion of privacy "harm" varies as some courts recognize those who have "suffered a concrete injury-in fact" as having standing to sue.[22] Meanwhile other courts recognize "economic and aesthetic injuries" such as the injury presented in *Spokeo* for standing purposes.[23] This apparent discrepancy in how courts recognize privacy as a harm causes inconsistent results throughout our country's legal system. Therefore, the NTIA should be more transparent as to what types of harm qualify as privacy harm for which one can recover under the law in developing a voluntary risk-based Privacy Framework.

It is important to note that these comments do not suggest that the NTIA, "furnish a new definition of privacy, nor catalogue the many values that privacy protects."[24] Instead, the NTIA should distinguish "privacy harm as a unique type of injury with its own characteristics and

[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 INDIANA LAW JOURNAL.

mechanisms."[25] By distinguishing privacy harm in this manner, the NTIA can help construct "a defensible means by which to rule out and recognize privacy harms."[26] In other words, the NTIA can help prevent ambiguity in the law when cases such as *Spokeo v. Robbins* and *Curry v. AvMed* arise.

One strategy the NTIA can take when trying to resolve the ambiguity that exists in the law in terms of privacy harm is to distinctly identify the boundaries of privacy harm.[27] By distinguishing the boundaries of privacy law the NTIA's Privacy Framework will be of "practical use to scholars, courts, and regulators attempting to vindicate and protect privacy and other values."[28]

One way the NTIA can distinguish the boundaries of privacy harm is by characterizing the types of harm through a categorical approach. Under this approach, privacy harms may fall into either "a subjective or objective" category.[29] Such categorization enables the types of harm to coexist while remaining separate.[30] In other words, each harm can occur without the other.[31] On one hand, harm may be "subjective" in that it is internal to the person harmed.[32] This type of harm generally stems from unwanted observation and can be inflicted on one person or many people. Subjective harm can range from one experiencing slight discomfort to extreme mental pain and distress.[33]

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*

On the other hand, privacy harm can be categorized as "objective" or as being external to the person harmed.[34] The type of harm that can be classified under this category "involves the forced or unanticipated use of information about a person against that person."[35] This type of privacy harm can be seen in circumstances when personal information is used as means to justify an adverse action against that person. An example of this can be seen when the government uses sensitive personal information to block a citizen from air travel.[36] Objective harm can also take place when sensitive personal information is used to commit a crime such as identity theft.[37] The two types of harm can be distinguished in that objective privacy harm is the adverse consequence such as the actual theft of one's identity. Meanwhile, subjective privacy harm is based on one's perception of loss of control which typically results in fear or uneasiness.[38]

There are many advantages to the NTIA recognizing that privacy harm is a harm and that different types of privacy harms can fall into two distinct categories. An important advantage is that this system can capture a complete range of harms.[39] Since this categorical approach in identifying privacy harm as a harm will cover the scope of harm, it enables a manner for ranking the "relative severity of privacy harm."[40] The NTIA should consider this system when developing a Privacy Framework as it will help to establish privacy harm as a distinct injury while also identifying its particular bounds and properties.[41] Courts then can have a more transparent approach when evaluating if the alleged harm constitutes as an actual privacy harm and if one should recover under the law. This approach can have an even greater impact if the NTIA were to

[34] *Id.*
[35] *Id.*
[36] *See Id.*
[37] *See Id.*
[38] *See Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*

achieve its high-level goal of harmonization through federal action. In other words, harmonized national data protection law could apply across every state and set the boundaries of privacy harm.

II. Harmonization

One of the NTIA's high-level goals for federal action is to harmonize the regulatory landscape. While the NTIA recognizes that the current sectoral system that is in place provides "strong, focused protections and should be maintained," there needs to be a legal system in place that avoids duplicative and contradictory privacy-related obligations placed on organizations.[42] As the NTIA points out, the sectoral or "patchwork" system that is currently in place fails to improve privacy outcomes for individuals who may be unware of their privacy protections depending on where they live. By implementing a harmonized regulatory landscape, the United States can help ensure organizations that process personal data are flexible, strong, and predictable in their approach.

As the NTIA stated the United States current sectoral system provides strong focused protections. For example, in California, the California Consumer Privacy Act of 2018 allows for citizens to propose "new laws and constitutional amendments."[43] This law also grants consumers four basic rights including the right to know what personal information a business is collecting, the right to "opt out" of allowing a business to sell personal information to third parties, the right to have a business delete their personal information, and the right to receive equal service from a business.[44] However, it is important to recognize that this array of new rights is only afforded to

[42]Developing the Administration's Approach to Consumer Privacy, FEDERAL REGISTER (2018), https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy (last visited Nov 6, 2018).

[43] The California Consumer Privacy Act of 2018, PRIVACY LAW BLOG (2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of- (last visited Nov 5, 2018).

[44] *Id.*

California residents under this law. However, if implemented as a federal regulations it could have much broader implications.

When looking for ways to implement a harmonized privacy policy in the United States, the NTIA should look to Europe's General Data Protection Regulation (GDPR) as a model. The GDPR is a law that aims to provide control to individuals over their personal data. It strives to simplify data protection by unifying the regulation within Europe.[45] The European Union decided that one major way it could enhance harmonization was to enact the new law in the form of a regulation opposed to another directive.[46]This was strategic because a "regulation need not and cannot be transposed."[47] In other words, once the EU enacts a regulation, it is national legislation in each member state. Member states don't get the opportunity to depart from it through transposing legislation. [48]

Under the GDPR, there is not one EU data protection law. Instead, there are 28 national versions of data protection law derived from a common EU source.[49] While the GDPR is in by no means a perfect regulation, "it is a promising first step toward a new business culture that can become the norm."[50] The NTIA should consider the GDPR in its goal to create a harmonized landscape because it expands the scope of data protection laws.[51] In addition, a system like this

[45] *See* Privacy Perspectives | GDPR harmonization: Reality or myth? Related reading: Podcast: A discussion with FTC Commissioner Rohit Chopra, INSIDE THE EPRIVACY REGULATION'S FURIOUS LOBBYING WAR, https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/ (last visited Nov 4, 2018).
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law, BERKELEY TECHNOLOGY LAW JOURNAL (2018), http://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/ (last visited Nov 1, 2018).
[50]Michael Fimin, FIVE BENEFITS GDPR COMPLIANCE WILL BRING TO YOUR BUSINESS FORBES (2018), https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/#ab1bef1482f9 (last visited Nov 7, 2018).
[51] Arjun Kharpal, EVERYTHING YOU NEED TO KNOW ABOUT THE NEW EU DATA LAW CALLED GDPR CNBC (2018), https://www.cnbc.com/2018/03/30/gdpr-everything-you-need-to-know.html (last visited Nov 8, 2018).

helps hold organizations accountable as it drastically increased the penalties for non-compliance.[52] Unlike the United States current fragmented system, the GDPR minimizes organizations uncertainty about privacy law.[53]

It is important to recognize that if the United States were to implement a legal privacy framework, similar to that of the GDR there are several issues that could arise many of which fall under policy concerns. For instance, if a harmonized federal regulation is passed it could potentially be too narrow or too broad. If the law is too narrow, it could potentially leave out behaviors that should be punished under the law and thereby serve as less protective to consumers. For example, in cases of revenge porn, if the law is too narrow an individual may not be able to get justice.

This can be seen in the 2014 New York revenge porn case, *People v. Barker*. Here, the state law was too narrow to criminalize a man who shared naked photos of his girlfriend on Twitter by sending them to her boss and sister via email.[54] The Court held that the "defendant's conduct, while reprehensible, does not violate any of [part] statutes under which he is charged."[55] Meanwhile, if the government implements a legal privacy framework similar to that of the GDPR and it is too broad it runs the risk of being over inclusive such that it punishes people for behavior that should be lawful. If a broad privacy framework were to be implemented this may disrupt autonomy privacy or an individual's ability to conduct activities absent the concern of surveillance.[56]

---

[52] *Id.*
[53] *Id.*
[54] Joe Coscarelli, WHY NEW YORK'S FIRST 'REVENGE PORN' CASE ENDED TERRIBLY FOR THE VICTIM DAILY INTELLIGENCER (2014), http://nymag.com/intelligencer/2014/02/revenge-porn-not-a-crime-in-new-york.html (last visited Nov 4, 2018).
[55] *Id.*
[56] Autonomy Privacy, Information Privacy and Information Security Primary tabs, CODE OF CONDUCT | OFFICE OF ETHICS, https://ethics.berkeley.edu/privacy/pisi (last visited Nov 2, 2018).

While there are many hurdles that the NTIA must overcome in implementing a proposed approach on ways to advance consumer privacy. Receiving comments from the public allows for a productive dialogue which brings us that much closer to striking a balance between risk management and innovative advancements in the world of privacy.

Sincerely,

Caitlin Larke