9 November 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:

My name is Suzanne Allen and I am a second- year student at New York Law School. I am writing this comment in response to the request put out by the National Telecommunications and Information Administration (NTIA) on behalf of the Department of Commerce. As a student currently focusing on privacy, New York Law School has provided a platform which helped create a solid foundation to assist in developing a unique perspective to this Request for Comment (RFC).

The NTIA is requesting comments seeking ways to advance consumer privacy through a user-centric approach. The RFC stresses the need to ensure the protection of innovation and prosperity and creating a comprehensive policy that will not stifle smaller businesses or those that collect less information. The RFC properly acknowledges the need for trust at the center of these privacy policies. Without trust, privacy policies will always fall short and fail to protect consumers. The breaches that have occurred within the last two months alone have made it clear that companies have a lot of work to do in order to win back the trust of their consumers. The NTIA acknowledging through this RFC that, as they currently stand, our policies are not sufficient in order to adequately safeguard the average consumer creates hope that we as a country can move further in the right direction.

While the privacy outcomes listed in the RFC are important to the Administration's discussion of refocusing consumer privacy in the United States, the bulk of this comment will focus on one of the high-level goals for federal action. The first point this comment will address transparency as one of the RFC's privacy outcomes and how companies can work towards being transparent through this proposal. The second point this comment will address is accountability as a privacy outcome and how important it is that companies be held responsible for what they do with consumer data.

The remainder of the comment will focus on the RFC's first high-level goal to harmonize the regulatory landscape. It will discuss the pitfalls of a patchwork framework and the broad outline which the Administration seeks to set forth. It will look to what the goal is hoping to achieve and what the Administration can do in order to further that goal by looking to fill in the gaps.

Privacy Outcomes: Transparency

Arguably one of the most important privacy outcomes listed in this RFC is transparency. The RFC correctly states that users should be able to easily understand how companies collect, store, use, and share our data. This is a key goal in order for companies to continue thriving in an age where users are feeling less and less safe sharing their information. The lack of safety or better phrased, the lack of trust, a consumer feels when they engage in activity online, is the central problem with today's regulatory framework.

The current regime has been built on the standard of notice-and-choice, which poses a problem for transparency. The bedrock principles of notice-and-choice are that company is required to notify its users about what data will be collected and the manner in which the

company will be collecting, using, storing, or sharing data.[1] Once a company provides notice, consumers are permitted to choose whether they want to continue to use that service, find another service to use, or decide against using a service at all.[2] The issues presented by notice-and-choice are, generally put, twofold: notice can never truly be adequate, and we are not in a position to opt-out of every service which collects our data because technology is an indispensable part of today's society.[3]

Notice to consumers generally comes through a privacy policy issued by a company. This, however, does not suffice as adequate notice. Anyone who has ever clicked the "read more" button to actually read a privacy policy knows that they are hopelessly long and difficult to understand.[4] This causes most people to choose not to read privacy policies at all because the point is moot: if you cannot understand it there is no reason to waste time trying. One software company even went so far as to hide a cash prize within their privacy policy available to anyone who noticed the clause and sent them an e-mail.[5] More than 3,000 people agreed to the policy without reading it, forfeiting a $1,000 prize.[6]

Perhaps companies purposefully structure privacy policies this way so no one will attempt to read them. Companies may feel that if fewer people read privacy policies, fewer people will realize if and when something has gone awry. But this cannot and should not be the standard to which companies are held. The RFC recognizes that privacy policies are often

[1] Waldman, Ari Ezra. Privacy as Trust: Information Age (pp. 79-80). Cambridge University Press.
[2] Waldman, Ari Ezra. Privacy as Trust: Information Age (pp. 80). Cambridge University Press.
[3] Waldman, Ari Ezra. Privacy as Trust: Information Age (pp. 83, 85). Cambridge University Press.
[4] Waldman, Ari Ezra. Privacy as Trust: Information Age (pp. 84). Cambridge University Press.
[5] Richard Beaumont, Transparency Should be the New Privacy, International Association of Privacy Professionals (May 14, 2014), https://iapp.org/news/a/transparency-should-be-the-new-privacy/.
[6] Id.

lengthy and inadequate but fails to offer a way to remedy this. This comment proposes a shift in the regulatory regime as a solution: moving away from notice-and-choice.

In order for companies to be transparent, companies should begin to move towards acting with privacy-as-trust in mind. Privacy-by-trust is an attempt to recognize that companies have a major leg up on their consumers.[7] It works within notice-and-choice as a mechanism not only to strengthen the disclosures we are getting upfront, but by going beyond initial disclosure.[8] While this shift in regime is not a clear-cut solution to the problems posed by transparency, it will create more transparency on behalf of the company and help consumers trust the services they are using.

The Administration recognizes the importance of transparency moving forward. But transparency should ultimately boil down to consumers trusting the companies with which we engage every day. Trust is successfully used as the standard in a number of other industries, and there is no reason privacy cannot be one of them.

Privacy Outcomes: Accountability

The concepts of transparency and accountability are heavily intertwined. Many companies are less than satisfactory when it comes to transparency. This, in part, might be due to the fact that companies are nervous that if they tell us exactly what they are doing with our data, that we will be more likely to hold them accountable for when that data is used for other purposes. In addition, if companies are not clear about what is happening with our data once it is collected, we will be less likely to realize when it is being used improperly- unless we are notified of an actual breach at the discretion of the company.

[7] Waldman, Ari Ezra. Privacy as Trust: Information Age (pp. 79). Cambridge University Press.
[8] Waldman, Ari Ezra. Privacy as Trust: Information Age (pp. 85). Cambridge University Press.

Companies cannot be properly held accountable unless they are transparent. As previously stated, consumers are already at a disadvantage when it comes to dealing with the companies collecting our data. We are subject to whatever methods they deem necessary in order to run their business. A company could be extremely transparent and vow to act in trustworthy manner, but the third-parties to whom they are inevitably selling our information may have made no such promises.[9] Who is held accountable in this scenario? It is unlikely the company would be held accountable over the third-party in this situation because it was transparent and did not misuse the data it received. The only solution would be to begin holding companies accountable for selling or sharing our data with third-parties who do not hold themselves to the same privacy standards.[10]

The trust that we as consumers have in companies should be grounded in something other than the fact that we are all but forced to engage with these companies daily. This trust should stem from accountability. Instead of only being held accountable when a company fails to inform consumers that data was used in a certain way, knowing that companies will be held responsible for using data in a way it was never meant to be used will create trust amongst consumers. Companies should not be able to take advantage of the fact that we rely on them in order to capitalize profits at our expense. Consumers should feel confident and trust not only the company with which they are interacting, but also those responsible for ensuring that companies are held accountable for their actions.

[9] Jack M. Balkin & Johnathan Zittrain, A Grand Bargain to Make Tech Companies Trustworthy, The Atlantic (Oct. 3, 2016), www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346.
[10] Waldman, Ari Ezra. Privacy as Trust: Information Age (pp. 87-88). Cambridge University Press.

High-Level Goal: Harmonizing the Regulatory Landscape

The RFC States that there are competing baseline laws throughout the United States. It further states that this patchwork framework creates harm within the American economy which ultimately harms consumers because they are unaware of what protections they have depending on the state in which they live. Complying with multiple regimes of law is an issue that many companies, mostly larger ones, are already being faced with due to the recent implementation of the California Online Privacy Protection Act (CalOPPA) and the General Data Protection Regulation (GDPR) in Europe.

The idea that we as a country should have broad overarching goals that can be modified slightly state-by-state is not too dissimilar from how the GDPR operates. First and foremost, the structure of the GDPR allows for data protection to be a fundamental right.[11] However, unlike the European Union, the United States is currently lacking a nationwide privacy policy. Instead, there are only four federal privacy laws which apply to certain sectors of people's lives- like our medical information or information which is held by financial institutions.[12]

Additionally, an approach similar to the GDPR would likely have the effect desired by the Administration. The European system functions inherently differently than the notice-and-choice regime used in the United States by building consumer protection from the beginning by ensuring that each entity involved in a transaction is complying with the regulation.[13] There is a vast difference between a regime that gives you the option to opt-in to something rather than opt-

[11] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation): Compromise Amendments on Articles 1-29, COM (2012) 0011 (Oct. 7, 2013).
[12] Ari Ezra Waldman, Privacy, Notice, and Design, 21 Stan. Tech. L. Rev. P74.
[13] Manu J. Sebastian, The European Union's General Data Protection Regulation: How Will It Affect Non-Eu Enterprises?, 31 Syracuse Sci. & Tech. L. Rep. 216.

out. As a consumer, it means you would have to give explicit consent for companies to collect your data rather than data automatically being collected unless you withdraw consent.

The sectoral based approach currently implemented in the United States implies that data protection is only something people have a right to in certain scenarios. With how much the Internet has grown and expanded throughout the years, there is no reason that data protections should not be implemented in areas other than the specific sectors currently protected by United States federal law. Consumers today lack the "choice" to use the Internet or the countless services that collect data. These services are woven into our daily lives and play a constant role in the decisions we make. To deny consumers protection in their daily lives, from companies who arguably know more about us than our health provider ever will, is simply illogical.

Implementing something similar to the GDPR would likely be the best way for the Administration to harmonize our regulatory landscape. It would encourage companies to act with the interests of their consumers in mind and be cognizant of the practices in which they engage. Additionally, the GDPR is already affecting any company in the United States that does business in Europe. This means that many companies are already in compliance with the GDPR out of necessity, lest they lose their international business.[14] This goal aligns perfectly with the two privacy outcomes discussed previously. If there is a national regulatory privacy framework, it will create transparent companies who will also be held accountable when their practices are less than satisfactory.

The RFC correctly states that there would be some difficulty in applying a nationwide specific law to companies of varying sizes. Small companies that do business in California or

[14] Manu J. Sebastian, The European Union's General Data Protection Regulation: How Will It Affect Non-Eu Enterprises?, 31 Syracuse Sci. & Tech. L. Rep. 216.

Europe are being forced to alter their practices and procedures unless they are willing to risk losing those markets altogether in order to evade compliance. This can undoubtedly put small companies in a difficult position: spend money to comply with strict privacy rules or lose out on some of the largest economic markets by restricting services to consumers in other areas. Without the resources that large corporations have smaller companies could be put at a disadvantage.

However, many smaller companies do not collect nearly as much data as large corporations, so there would be less with which they would need to comply. In addition, more often than not, smaller companies are not collecting the same type of data that large corporations are collecting for the same reason they would have a hard time following stricter laws: they do not have the funds to do so. It is important to keep this in mind when trying to develop a regulatory framework by which we as a country could abide.

The administration appears to be attempting to avoid this problem by setting forth broad goals instead of concrete policies. While this approach would undoubtedly have positive effects, the proposal being broad ignores some potentially serious problems. Under this approach, companies could do virtually nothing in order to protect their consumers because there would be no real way to enforce a policy that does not exist. While there would be some hope if consumers could show that a company did not do one specific thing- like the company was not transparent in how it collected, used, and shared data- all a company would have to do overcome this is show that it made a mere attempt to be transparent.

For example, one company created an internet-connected thermometer which syncs to an app to allow users to input their symptoms when they are sick in order to track those

symptoms.[15] That company is selling the data to another corporation that sells disinfecting products so it can use the data to target ads to the zip codes showing the most users with flu-like symptoms.[16] Amazon was recently granted a patent application allowing them to recommend soup or cough drops when an Amazon Echo detects coughing or other symptoms while the user is speaking to the device.[17] Various smart TV brands have contracted with a third-party to allow the third-party to prompt users to opt-in to their service while setting up their new TV. The third-party says it will allow users to "get recommendations based on the content you love" and "engage with your TV in a whole new way," when in reality the third-party is tracking the networks, ads, and even which video games are played on the TV.[18] It can tell how many devices are connected to the same wireless network, and then targets all of those devices with ads based on the content which was played or watched on the TV.[19]

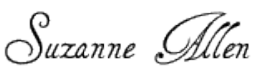
Situations such as these are becoming increasingly common as technology continues to advance and consumers desire more from their devices. These situations raise not only privacy questions, but ethical questions as well. Despite the fact that these companies are technically acting in a privacy-compliant manner, is what they are doing really right? This is where a uniform regulatory regime comes into play, and what the Administration should be focusing on. Without a uniform standard to which companies can adhere, they are essentially left to make the rules for themselves.

---

[15] Sapna Maheshwari, This Thermometer Tells Your Temperature, Then Tells Firms Where to Advertise, New York Times (Oct. 23, 2018), https://www.nytimes.com/2018/10/23/business/media/fever-advertisements-medicine-clorox.html.
[16] Id.
[17] Id.
[18] Sapna Maheshwari, How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight, New York Times (July 5, 2018), https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html.
[19] Id.

Thank you for the opportunity presented by participating in this request for comments. your time and consideration are greatly appreciated.

Sincerely,



Suzanne Allen