Final Exam # 7190

November 9, 2018

David Reidl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce

Via email to: privacyrfc2018@ntia.doc.gov

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

As a second-year law student currently enrolled in an Information Privacy course, I am pleased to submit these comments in response to the National Telecommunications and Information Administration's ("NTIA") request for public comments ("RFC") on ways to advance consumer privacy while protecting prosperity and innovation.

While it is commendable that the administration is concerned with advancing consumer privacy, it is difficult to address many of these concerns without enacting a comprehensive consumer privacy law in the United States ("U.S."), like the European Union's General Data Privacy Regulation ("GDPR") which went into effect on May 25, 2018, or the recently enacted California Consumer Privacy Act of 2018 ("CPA") slated to take effect on January 1, 2020.

In 2017, nearly 179 million records were exposed from 1,579 data breaches in the U.S.[1] In fact, the largest data breach to date was reported in 2016 when online platform Yahoo announced hackers stole user information related to at least 1 billion accounts in 2013.[2] Earlier this year, Equifax reported the extent its 2017 data breach.[3] The breach exposed sensitive data

[1] The Statistics Portal, *Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions),* STATISTA (2018), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
[2] *Id.*
[3] Alexa Johnson, *Equifax Breaks Down Just How Bad Last Year's Data Breach Was,* NBC NEWS, (May, 8, 2018, 7:25 PM), https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496.

including thousands of passports and drivers licenses along with the Social Security numbers of more than 146 million consumers. The reality is that data breaches are happening to the organizations we have entrusted with our most sensitive information and these data breaches are increasingly serious because our data is constantly being collected.[4] Consequently, it is not surprising that the latest NTIA survey found most Americans continue to have privacy and security concerns.[5]

My comments will focus on feedback regarding some of the core privacy outcomes that consumers can expect from organizations. I will discuss ways the administration can ensure these outcomes can be achieved and what is missing from many of the expectations consumers should have of the organizations with respect to data. I will also discuss how the different parts of the GDPR and the California Privacy Act can also help guide the administration's efforts to focus on consumer privacy while promoting innovation, and how the current notice-and-choice system is not effective in protecting consumers.

The GDPR

The GDPR has seven fundamental principles at its the foundation. These principles regulate the way that data is controlled and processed by both public and private organizations. They are: (1) lawfulness, fairness and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality (security); and

[4] Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES, (May 21, 2018, 12:42 AM), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#37368a5e60ba.

[5] Rafi Goldberg, *Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds,* NAT'L TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION: BLOG, (August 20, 2018), https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds.

(7) accountability.[6] The objective of the GDPR is to minimize the risk of data breaches by strengthening the mechanisms that protect personal data.[7]

A critical change in the law is the viewpoint that personal data is owned by the individual and not those controlling or processing. In the *Charter of Fundamental Rights of the European Union*, which became legally binding in 2009, two fundamental rights afforded to citizens is the right to privacy and the right to data protection.[8] This is a departure from prior European law and from the U.S.'s view on data. Substantial attention should be paid to these fundamental principles because failure to comply with the GDPR may result in substantial fines and penalties.[9]

U.S. companies without any physical presence in the European Union could be subject to obligations under the GDPR because the GDPR encompasses companies that collect or process the personal data of European Union citizens.[10]

The CPA

The CPA was enacted in June 2018 and is similar to the GDPR in that is focuses on consumer privacy from the point of view of the consumer and tries to put the consumer in control of his personal data. The CPA has four main provisions: it gives consumers (1) the right to know what personal information a business has collected about them, where came from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold; (2) the right to "opt out" of allowing a business to sell their personal information to third

---

[6] GDPR at Art. 5 § 1.
[7] Todd Ehret, *U.S. Firms are Still Unprepared for Looming EU Data Privacy Rules*, THOMSON REUTERS (Feb. 13, 2018), https://www.reuters.com/article/bc-finreg-data-privacy-rules/u-s-firms-are-still-unprepared-for-looming-eu-data-privacy-rules-idUSKCN1FX2D2.

[8] The Charter of Fundamental Rights, Title 1, Art. 7
[9] GDPR at Art. 83 § 3.
[10] *See* GDPR Art. 2-3.

parties; (3) the right to have a business delete their personal information; and (4) the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the CPA.[11]

The CPA also imposes penalties on organizations that fail to comply. The CPA provides a private right of action that allows consumers to seek damages both actual or injunctive against an organization that if their sensitive personal information is subject to unauthorized access, theft or disclosure as a result of a business's failure to implement and maintain required reasonable security procedures.[12]

The CPA has the potential to change the landscape of U.S. privacy law because it protects California-based consumers, regardless of where the organization has its principle place of business. Section 1798.40 (7)(g) of the CPA defines a California-based consumer as "a natural person who is a California resident."[13]

Core Privacy Outcomes

Transparency

Users should be able to understand not only how but when an organization collects, stores, uses, and shares their personal information. Although organizations use privacy policies to give users this information, they are ineffective to promote transparency because they are almost always lengthy and difficult to understand. So much so that a company hired a former

[11] Kristen J. Matthews, Courtney M. Bowman, *The California Consumer Privacy Act of 2018,* PROSKAUER ROSE LLP: PRIVACY LAW BLOG, (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.
[12] *Id.*
[13] CPA § 1798.40 (7)(g)

radio show host to read its privacy policy and turn it into a sleep story.[14] In addition, privacy policies are usually plagued with issues like promising never to share data when almost all organizations outsource at least some functions to third party contractors or vendors.[15] Transparency should be a basic function of internet use and a privacy policy that consumers do not read or understand is equivalent to providing no protection.[16] Thus, any form of consumer privacy reform should include not simply guidance or recommendations, but also mandates to ensure transparency is adhered to from the developmental stages of writing privacy policies.

Article 12 of the GDPR requires organizations to take appropriate measures to provide information relating to processing to users in a "concise, transparent, intelligible and easily accessible form, using clear and plain language."[17] The information must be provided in writing, by electronic means, and if a user requests, orally.[18] Known as the "right to be informed," the GDPR gives consumers the right to be informed about the collection and use of their personal data.[19]

Section 1798.100 (b) of the CPA also has similar stipulations as it requires a business that collects a consumer's personal data to inform them about which categories of or personal information is going to be collected at for what purpose.[20]

---

[14] Bill Murphy, Jr., *Privacy Policies are Boring. This Company's Answer is Brilliant,* INC. (May 31, 2018), https://www.inc.com/bill-murphy-jr/privacy-policies-are-boring-this-companys-answer-is-brilliant.html.
[15] Saad Gul and Michael E. Slipsky, *10 Problems that Plague Privacy Policies,* LAW 360 (September 19, 2016), https://www.law360.com/articles/841387/10-problems-that-plague-privacy-policies.
[16] Center for Plain Language, Privacy-policy Analysis at 1. https://centerforplainlanguage.org/wp-content/uploads/2016/11/TIME-privacy-policy-analysis-report.pdf.
[17] *See* GDPR Art. 12.
[18] GDPR at Art. 7.
[19] GDPR at Right to be Informed.
[20] CPA § 1798.100(b)

The NTIA should consider passing regulations that include similar requirements with respect to transparency. As a threshold matter, organizations that process, collect, store, or sell consumer data should tell users how and when the data is being used. The language in the proposed outcomes included in the RFC is alarming because it does not give enough guidance to organizations on what it should provide to users and how.

Control

Internet users should be able to exercise control over the collection, use, storage, and disclosure of the personal information they provide to organizations. In the U.S.'s current notice-and-choice process, organizations often take the view that internet users have control over their data because they can choose to use a different platform once they are given notice about an organization's privacy policy. Essentially, notice-and-choice was designed to allows users to control personal data by deciding whether users would like to disclose personal information to a particular organization.[21] However, the constant collection of data from different sources makes it difficult to truly control the dissemination of our information. Additionally, users freely give information for legitimate purposes, and that information is often sold to third parties.

Organizations usually obtain information in two primary ways. One way is to receive the information directly from the internet user. The second way is to obtain the user's information from the third party. With this in mind, the Articles 13 and 14 of the GDPR requires organizations to provide different types of information, depending on how the user's data was collected. Article 15 is the right to access and allows the data subject to access any information the organization has collected from user. Article 17 deemed "the right to be forgotten," allows users to get from the organization the "erasure of personal data concerning him or her without

[21] Ari Waldman, *Privacy as Trust: Information Privacy for an Information Age* 32-33 (2018).

undue delay." In fact, Chapter 3 of the GDPR lists all of the "Rights of the Data Subject," that is, the identified or identifiable natural person whose data has been collected.[22]

The CPA has a similar approach. Section 179.100(d) requires a business that receives a request from a consumer to promptly provide the consumer with access to the personal information, free of charge to the consumer. Section 1798.105 (d) gives consumers the right to have a business delete their personal information, although there are some exceptions. Additionally, consumers have the right to "opt-out" of a company's practice of selling its personal information to third parties.

The requirements of both the GDPR and the CPA make is clear that the focus is on giving the consumer control of his personal data. This is more comprehensive than notice-and-choice because not only are there requirements on what the "notice" should be, there are provisions that put the control in the hands of the consumer and gives the consumer practical options of data control, not a simple "I Agree" button as you gain access to a website.

The NTIA should consider revising its control outcomes to include regulations that mandate organizations to actually allow users to control the use, dissemination, processing, and selling of personal data.

Security

Organizations that collect, store, use, or share personal information should employ security safeguards to secure these data. Internet users should expect that their data are protected from disclosure, breach, loss, or modification. At the heart of many data breaches in inadequate security. Even if data collection is transparent, and consumers freely give their data to organizations, if an organizations security measures are subpar, data breach becomes inevitable.

[22] GDPR at Art. 4.

In addition, an organization's security should also extend to its third-party vendors. One notable example is Target's 2013 data breach. During the investigation, it was discovered that the breach likely occurred due to the hackers penetrating Target's network through the compromised credentials of a third-party vendor.[23]

One way the GDPR tackles security is by mandating that data controllers or processors designate a data protection officer to ensure that the organization is in compliance with the GDPR and to be the point person, within the organization, who communicates with the GDPR's supervisory authority.[24] The controller or processor must also ensure that the data protection officer stays abreast of all issues relating to the protection of personal data.[25] Additionally, the data protection officer is tasked with communicating with data subjects about issues relating processing of their personal data.[26]

The position of the data protection officer is crucial because it makes an expert responsible for compliance with the GDPR. By including this provision, the GDPR not only creates jobs, the GDPR designates at least one person to ensure that the security is a priority for the organization.

Although the CPA does not require businesses to create a data protection officer role, businesses are required to remain compliant with the CPA. Due to the requirements of the CPA and the fact that it is the first law of its kind in the U.S., implementation and compliance will likely require organizations to employ experts to not only ensure that organizations are securely

[23] Xiaokui Shu, Ke Tian, Andrew Ciambone, and Danfeng Yao, *Breaking the Target: An Analysis of Target Data Breach and Lessons Learned at 2*, https://arxiv.org/pdf/1701.04940.pdf.
[24] GDPR at Art. 39.
[25] GDPR at Art. 38.
[26] *Id.*

handling consumer data but also to ensure third-party vendors are implementing robust security measures.

Users should expect their information to be secure, and the NTIA should be proactive in enacting regulations that require organizations to implement specific security measures. The NTIA should define what "securing" personal data means and what the appropriate levels of security should be for different organizations—or if all organizations are required to have the same level of security. Does security mean encryption? Does it mean using security keys? Without proper requirements, the NTIA will allow organizations to define these terms and systems, continuing the proliferation of data breaches in the U.S.

The list of general outcomes, although, a good start is simply not enough to ensure organizations will oblige. The reality is, unless a comprehensive consumer privacy law is passed in the U.S., organizations, particularly some that do not have to process, share, or store data from European citizens, internet users will continue to be concerned with internet privacy. The free flow of information is important to the function of our society and having little to no control over your own data should not be an impediment to benefitting from the value of the internet of things.

Innovation Concerns

Users should not be forced to choose between good technology and privacy. Although balancing interests of technology companies and consumer privacy is a starting point, putting innovation ahead of privacy is putting the proverbial cart before the horse. Privacy should be a consideration at the outset of technological advances. Unfortunately, as consumer concerns about

privacy have increased, and the risks of data breach and data theft have also increased.[27] One reason is because many governments have not implemented proper strategies to address these concerns and have left it up to notice-and-choice, a mostly self-regulatory system.[28]

The NTIA should work on implementing policies like privacy by design, which would certainly require an offensive look into privacy, rather considering it after designing the technologies of tomorrow. Privacy by design can be beneficial because technology companies are the experts and more equipped with the tools to consider privacy early in the process. Privacy by design would also be helpful in resolving the issue of consumers rarely reading privacy policies and forces organizations to not only take technical steps, but to make organizational changes to incorporate privacy.

The NTIA may also want to incorporate licensing and ethics requirements for technologists. Many industries, require their members to undergo ethical training and licensing requirements when they have to handle sensitive client information. Technologists may benefit from training on considering privacy early in the development process.

[27] Marc Rotenberg, *Promoting Innovation, Protecting Privacy,* OECD OBSERVER, (2016), http://oecdobserver.org/news/fullstory.php/aid/5593/Promoting_innovation,_protecting_privacy.html.
[28] *Id.*