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

Docket No. 180821780– 8780–01

Dear Mr. Travis Hall,

I am a law student from New York, I want to thank you and the National Telecommunications and Information Administration for the opportunity to comment on such a pressing and prevalent issue. Having witnessed all the rise of technology and now all the areas impacted by privacy concerns I appreciate how important and complex the matter is today. I will be addressing the issue of Harmonizing the Regulatory Landscape.

If we seek to harmonize privacy regulations while promoting the American economy, we need regulations that promote broad enough principles to cover all industries and specific enough to identify when there is a breach of privacy. If the interest is to promote innovation and business while improving privacy outcomes we must enforce consumer confidence by providing a basis for trust. While privacy is not laid out directly in the constitution our common law has articulated an implied right to privacy. Through the 4th Amendment's "reasonable expectation of privacy" doctrine and the "right to be let alone" as articulated in ***Olmstead v. United States***, 277 U.S. 438 (1928) we have come to recognize privacy as a right. It is trust that promotes innovation, when consumers believe that the information they are sharing with companies will be handled in manner in which their interest are protect they engage in the market. As the data breaches of

2018 have shown us consumers will walk away from companies that mishandle or fail to protect their personal information. [1]

The European Union recently enacted the GDPR[2] which protects any information (of a European Union citizen) that can be classified as personal or identifying information. Even companies not based in the EU must comply if they collect, process, or store data of an EU citizen. US privacy law is fragmented and has not adequately kept pace with technology. Privacy has been defined by what is reasonable "expectation of privacy", but it is time to reframe that definition. The technological has boom has left a lot of legal and societal confusion as to what is reasonable. The GDPR can serve as an example of how harmonization can start to dispel confusion in the law and increase consumer confidence. While some criticism about the GDPR's clarity it should be acknowledged that the broad language is intentional as the purpose is to capture those technologies that have not developed. In centering the provisions around protecting the individual and presenting what conduct would place a duty on the company to the consumer.

The United States should shift their focus from imposing the burden on the consumer to safeguard their own data and instead hold those who collect, store and distribute data accountable. Three problems exist with the policy that consumers should be accountable with whom they share their data. First, technology has become an integral part of the average person's life and their ability to participate in society hinders on the use of technology. This takes away from their ability opt out because in doing so they seriously hinder their ability to access basic services like finances/banking, health and communications (email, cellphone). Second, the average consumer does not know how, when or what is being collected, stored or shared.

[1] https://www.techradar.com/news/nearly-one-in-10-us-facebook-users-have-deleted-their-accounts-survey-says
[2] https://eugdpr.org

Consumers do not know when their data is being shared or sold to third parties and for what purposes. In the Dwyer v. American Express Co. 273 Ill. App.3d 742 (1995) the company tracked their clients spending habits then sold that information to marketing companies. The plaintiff's faced several issues in their claim including that the act of using the financial institution's service, a credit card, they had consented to the collection. The court found that Amex had not disclosed to consumers that it would be selling information about their spending habits to third parties however plaintiffs failed to show harm and could not recover. Companies and large institutions provide consumers with terms of service and its privacy policy that inform them of their policies. However, these contracts and notices that consumers are agreeing to are presented in a manner that does not foster true consent. They are often long documents, filled with legalese in font that is remarkably small. Consumers are signing away their data including sensitive information without being fully informed. Third, the company knows exactly how a consumer's data is collected, maintained and shared. They can also better appreciate the risk that the consumers are facing when they send their information. While companies like Google[3] have argued that consumers should expect that in using their email service their electronic communications would be scanned and its contents expose to the company. An unsettling feeling that the court experienced was felt and Google's argument was rejected. They maintained that much like a letter sent in the mail the sender and recipient were not private information but that the contents remained private. The Supreme court has been able to stretch common law principles to some new technologies, but the pace at which information is shared has increased and the doctrine does not safeguard information voluntarily provided to third parties. The court

[3] https://archive.nytimes.com/www.nytimes.com/interactive/2013/10/02/technology/google-email-case.html

has continually pointed out the need for congress to fill in the gaps in the law.[4] Recognizing privacy as a right or expanding its protections is paramount to maintaining the balance between consumers and industries in which there is a large power gap.

Federal and state legislatures have attempted to regulate and reigning the conduct of companies that seek to exploit its consumers. In 1968 congress created Electronic Communications Act which was an update of The Federal Wire Tap Act. It reflected the new technologies that no longer required "hard" telephone lines. This older definition did not cover electronic communications that were newly developed. By using this broader language congress sought to capture any new or future technologies that would amount to an electronic communication. This same approach could strengthen harmonization by using broader terms to define private information and privacy violations and diminish the need for a sectoral system.

Privacy issues can be improved by establishing a Federal level baseline of principles and regulations enforceable by the FTC. These principles should be built on commonly accepted foundations of US privacy law. The sectoral approach we are currently practicing provides a unique approach to each industries complexity. However, we have reached an impasse in which all types of personal information are liberally shared by the consumer in order to participate in society. States like California have enacted protections that use broad language so as to capture all entities that collect or process data while shifting the burden onto those entities. However, the California Consumer Privacy Act is not the only state legislation regulating data in California. For example, the California Data Destruction Statute defines personal information more broadly including but not limited to home address, telephone number, identifiers allowing for physical or

[4] https://www.americanbar.org/groups/litigation/publications/litigation_journal/2013-14/spring/a_reasonable_expectation_privacy/

online contact and, passport number. Yet the California Data Protection Statute does not include in its definition of personal data home address, telephone number, identifiers allowing for physical or online contact and, passport number. This discrepancy in definitions adds to the legal confusion. In creating one principal data legislation with broad principles clearly defining the vocabulary, each party, their duties in processing, collecting, storing and distributing data, the penalties for breach or violations we can create harmonization between the states. Some states have addressed the issue similarly, both California and Massachusetts have strong consumer orient data protections. While others like New York focus on date security within financial institutions. [5]Definitions and standards vary across the states, some recognize personally identifiable information and biometric data while others address specific industries. Though the federal government should respect state sovereignty the need for guiding principles is highlighted by the fragmentation of data laws of the states.

These principles should remain sensitive to the fact that consumers are providing their personal information for a specific and limited purpose. The regulations should allow for the collection, transmission, and storage of data as is appropriate for the limited purpose prescribed by the circumstance in which the consumer provided the personal information. [6]In an era riddle with data breaches and mishandling of personal information consumer confidence should be restored. A large part of commerce takes place online and if consumers do not understand how their personal information is being used or who it is being shared with they will not participate as freely. Harmonization can provide the new standard and eliminate any doubts from consumers. Without harmonization would provide a means of tracking when a consumer's data is collected and when

[5] https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
[6] https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

it is destroyed. If states hold different requirements or are silent on destruction of data the consumer will not have certainty that a national corporation such as a bank has destroy their data.

In an era of inter-connectivity, we cannot confuse common sense regulations, now internationally recognized, as an impediment to innovation. The power imbalance from consumer to controllers, processors and third parties must be addressed before consumer confidence is lost. Why does an individual hand their financial institution personal information like their social security number? Because the expectation of privacy remains. As state by Justice Sotomayor "expectation would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *United States v. Jones 565 US 400 (2012)*[7] Harmonization would echo these principles as it would create a new standard of expectation of privacy, one not dictated or controlled by the fact that the individual has disclosed information and can better reflect the modern environment.

The sectoral approach is too fragmented and will continue adding to legal and societal confusion. It would not eliminate the issue that plague data privacy today like notice and consent. The privacy policy notices will either be incomplete for simplicity sake or remain too complex for the average consumer to understand. The courts will have to deal with the competing state laws. If harmonization is implemented as it has in the European Union with American principles like those in the California Consumer Privacy Act we can create an environment where there is transparency, trust and innovation.

[7] https://supreme.justia.com/cases/federal/us/565/400/