Adam Schwartz

Comments on Consumer Privacy

The concept of privacy and its evolution over recent years has left lawmakers in somewhat of a growing predicament, particularly when it comes to data security on the internet. The balancing act between consumer privacy rights and the ability of corporations to collect and transfer data has presented numerous challenges to legislators everywhere. As technology advances and companies are able to store a broader array of information on databases that are capable of holding an immense amount of information, the risk that is associated with a possible data breach increases significantly. For example, if a data breach occurs on one of these major databases, hackers can gain unauthorized access to the credit card information and home addresses of thousands of people at once.

The heightened focus on data security largely concerns "personally identifiable information" (PII). One of the main objectives of the GDPR is to protect against the wrongful disclosure of any information that can be used to personally identify an individual, especially when there is lack of consent from the individual as to the collection and usage of his/her data by a corporation. Although the GDPR does not specifically use the term "PII", the regulation is largely concerned with information that can be used to identify an individual. In fact, the GDPR places an outright ban on the processing of certain personal data that can be particularly damaging to an individual if wrongfully disclosed. Article 9 of the GDPR prohibits the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data

concerning a natural person's sex life or sexual orientation shall be prohibited.[1]" This omnibus approach to data privacy shown by the EU portrays its focus on preventing the breach of personal data, regardless of who is handling it. It also recognizes that although all PII is sensitive in some respect, there is some information so private and so personal that there should not even be a risk of wrongful disclosure of that information.

In the United States, the FTC has implemented a "notice and choice" regime as a response to data security concerns. The FTC has stated that it wants to ensure that consumers have the ability to make informed decisions pertaining to the handling of their PII. However, the FTC has also acknowledged that "companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer."[2] Based on this language, one may reach the inference that the FTC is hesitant to place such a strong burden on companies to inform consumers about the collection and usage of their data. While innovation is undeniably something that must be preserved for American companies to pursue, the advancement of technology and the ease with which massive amounts of information can be distributed calls for more protective privacy rights for consumers.

The "notice and choice" approach has unfortunately led corporations to form these absurdly long privacy policies that read like contracts. It is nearly impossible to expect consumers to read all of the privacy policies for every website they surf through. Therefore, the "informed consent" policy goal is being significantly underachieved. It cannot be reasonably asserted that consumers are making informed choices regarding the possible collection of their

---

[1] *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679. *See Article 9.*

[2] Internet of Things, Privacy & Security in a Connected World, at p. 40.

data if the information they need in order to make an informed decision is buried deep within the privacy policy that they are not going to read.

Tied in with the concept of notice-and-choice is the "opt-out" mechanism utilized by corporations as a way of giving the consumer a "choice" to decline the collection or sharing of their personal data. This opt-out process leads to another significant problem with the notice and choice regime, which is known as the "illusion of choice."[3] Companies may seem to be providing consumers with choice by installing this opt-out mechanism. However, in many instances, opting out would deprive the consumer of an essential service, which would negate the consumer's purpose for visiting the website in the first place. Corporations also deceive consumers by requiring consent for the use of personal data that is not actually related to the service being provided, which provides an avenue for corporations to engage in commercial transactions with personal data that the consumer did not consciously give permission for use.

Allowing corporations to collect and utilize consumer data before they provide choice to the consumer is essentially permitting these companies to engage in the formation of adhesion contracts. Assuming the consumer has already accepted the terms of the privacy policy, before the consumer has actually made a choice, goes against basic notions of contract law and informed consent. This issue would be less concerning if the FTC only permitted the collection of consumer data until the consumer is provided with choice. The fact that the FTC allows companies to go beyond collection and actually engage in commercial transactions with the personal data of consumers that have not yet consented is undoubtedly a hinderance on the privacy rights of individuals.

[3] http://www.lawtech.hk/pni/wp-content/uploads/2015/04/Fred-H-Cate.pdf *See 3. "Illusion of Choice"*

In order to more efficiently achieve the desired policy outcome of transparency between corporations and the consumers they attract, the United States should follow the footsteps of the GDPR and require companies to provide consumers with the option to "opt-in" to data collection processes. This change in how companies obtain consent from the consumer will have no impact on the commercial transactions that companies engage in upon getting approval. They will still be able to sell and transfer this data to other companies for marketing or other commercial purposes. An opt-in requirement would simply enable consumers to make a conscious decision with regards to the information they make available to the corporation.

Another problem with the current approach of the United States on privacy regulation is the variation between the different sectoral laws. The applicable privacy law varies depending on the industry. To illustrate, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to medical and health professionals, the Gramm-Leach-Bliley Act of 1999 applies to financial institutions, etc. This variation leads to gaps in protection, inconsistency, and uncertainty; particularly due to the nonstop evolution of technology and the data universe.[4] Laws often struggle to keep up with technological innovations due to the lengthy process of passing legislation in the United States. States may also pass different privacy laws through their respective state legislatures, such as the California Consumer Privacy Act of 2018 and Delaware Code §1204C. This lack of uniformity within privacy regulation makes it difficult to develop a common understanding about policy goals regarding privacy. Additionally, the variation of these laws makes it arduous for consumers to know what they are entitled to regarding their privacy rights and can pose challenges to corporations in terms of compliance.

[4] https://www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws/ *See "Consumer Privacy Bill of Rights"*

The most significant difference between the legislations of Europe and the United States on data privacy is that the GDPR is concerned with the nature of the data itself, whereas the federal legislation in the United States focuses on the nature of the company handling the data. This format of the sectoral system stands a barrier to the harmonization of privacy laws because instead of focusing on protecting the data of the individual, the laws instead act more as legal guidelines for professionals handling the data. For example, HIPAA only applies to particular entities. These entities are: (1) health care clearinghouses; (2) health plans; and (3) health care providers.[5] Gyms, health and fitness apps, certain health websites, massage therapists, banks, etc. are all examples of entities that handle health information to some extent but are not bound to the protections of HIPAA. If the privacy of the individual is the true concern, should it really matter what the nature of the company handling the information is? Any entity being trusted with such sensitive information pertaining to an individual should have a legal obligation to maintain proper safeguards against the improper or unauthorized disclosure of this health information. The possible harm experienced by the patient and the invasion upon their privacy remains the same, regardless of who is responsible for its misuse.

Quite possibly the most ambitious trait of the GDPR is that it is binding on companies outside of the EU if any of their online traffic comes from EU residents. This attribute of the GDPR has placed a hefty burden on American corporations because they are now being forced into becoming compliant with data security and privacy laws that are significantly more stringent than those of the United States. This could pose a threat to the growth of American businesses because GDPR compliance may deter companies from accepting EU traffic, which could cap the company's ceiling. Investors would then favor companies that could afford to achieve GDPR

[5] https://www.worldprivacyforum.org/2013/09/hipaaguide9-2/ *See "Other health record holders"*

compliance and accept EU customers, which could result in smaller companies taking daring and uncalculated risks.

The penalties for non-compliance with the GDPR can amount to $25 million or 4% of the corporation's annual income, whichever is higher. Such a heavy fine could obviously cripple a company beyond repair. Additionally, according to the Netsparker GDPR Survey (conducted in the EU), 92% of security executives working at an enterprise (more than 1,000 employees) predict that the costs of GDPR compliance will exceed $50,000, with around 25% estimating costs between $100,000 and $1 million dollars, and 10% estimating costs at over a million dollars.[6] This places an ultimatum on American companies in that they must decide between reforming their global data protection and data rights infrastructures to comply with the GDPR, or institute a patchwork data regime where Europeans are treated in a different manner than everybody else.

Article 6 of the GDPR highlights the requirement of Member States to establish at least one independent supervisory authority[7]. The purpose of these supervisory authorities is to make data breach reporting processes more efficient. By providing a government body that is responsible for monitoring data protection in each state, the EU has implemented a policy that benefits both the corporation and the data subject. The corporation benefits from having a concrete reporting system that can be utilized to prevent further liability for data breaches. The consumer benefits from the existence of an authority that serves as a "watchdog" over corporations handling personal data.

[6] https://www.netsparker.com/blog/web-security/gdpr-compliance-2018-survey-results/ *See "How Much Are Businesses Spending on GDPR Compliance?"*
[7] *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679. *See Article 9.*

Sadly, the establishment of the independent supervisory authorities has left another hurdle for American companies to face. There is no designated independent supervisory authority for the United States. In the occurrence of a data breach, American companies will be forced into contacting the supervisory authorities for each data subject in the EU. Meaning that if a breach occurs and the company accepts traffic from residents of every Member State to the EU, the company's Data Protection Officer (DPO) must contact the supervisory authorities in every Member State to report the breach. This burden results in petty expenses to the corporation, on top of being extremely stressful and time consuming.

One of the most essential objectives of the GDPR is to make data breach reporting processes faster and more efficient; and it effectively does so for European companies. However, the American companies trying to achieve GDPR compliance have to endure tedious expenses in updating privacy and internal data management policies, and exercise even more diligence when reporting data breaches. This diverts the attention of the company away from actual business activities, which could result in financial harm to the company and hinder success.

In order to achieve the policy goal of interoperability, there must be a change in how the United States governs data privacy. The EU has taken a more proactive approach in light of all the recent major data breaches across the modern world. If the United States is not going to pass federal legislation that is similar to the GDPR, lawmakers have to at least create an official entity tasked with compliance responsibilities. Perhaps the FTC itself can expand its own responsibilities pertaining to the proper enforcement of privacy rights.

Another route the FTC can take is to either expand on the Consumer Privacy Bill of Rights (CPBR) or pass a similar piece of legislation into law. The CPBR was drafted by the Obama Administration as a response to the recommendations put forth by the Department of

Commerce's Internet Policy Task Force in December 2010. The report stressed the importance of focusing on certain principles in regards to data privacy and security. These principles are as follows: (1) individual control; (2) transparency; (3) respect for context; (4) security; (5) access and accuracy; (6) focused collection; and (7) accountability.[8] When comparing these principles to the rights afforded to data subjects in the GDPR, the Consumer Privacy Bill of Rights seems to sympathize more with the interests of those handing consumer data, as evidenced by its mention of the "respect for context" principle. Although innovation may be somewhat stifled by turning these principles into law, American lawmakers may be able to use the "respect for context" principle to protect the ongoing creation of modern and innovative business models by American companies.

Finally, the concept of "privacy by design" should be another principle adopted and stressed by the FTC. So far, privacy law all around the world has failed to sufficiently prioritize the design processes of the equipment used to collect personal data. Instead, all of the focus is placed on the collection, use, and distribution of personal information. The data marketplace has become so competitive as technology has advanced that companies are constantly looking for more sophisticated equipment to collect the personal data of their customers. If more regulation were applied to the technological companies that developed data collecting equipment, it would lessen the incentive to invent such invasive equipment. There needs to be a shift in the mindset that companies need to collect as much data from customers as possible to create the best experience for them. Rather, protecting customer data privacy rights should be on the minds of both the technological developers creating new data collection devices, and the companies that are purchasing and utilizing this equipment.

[8] https://www.epic.org/privacy/white_house_consumer_privacy_.html

Professor Don Norman highlights the importance of privacy by design in his book, "The Design of Everyday Things". He advances an intriguing theory. He believes that the likeliness of new technology to be understood by the common person speaks to the quality of its design. When discussing the correlation between the complexity of the design and the ability of the user to understand the intended function of the technology, Norman writes, "Well-designed objects are easy to interpret and understand. They contain visible clues to their operation. Poorly designed objects can be difficult and frustrating to use. They provide no cues—or sometimes false cues. They trap the user and thwart the normal process of interpretation and understanding.[9]" Lawmakers should put some kind of pressure on technological engineers to adopt this mindset and develop less privacy-invasive instruments. This would also help develop a scale for the evaluation of data collection techniques and provide lawmakers with more tools to develop a better understanding of which techniques are more invasive, and which are not.

Although privacy by design is a forward-thinking concept and should be considered by all developers of technology as well as lawmakers in charge of regulating such development, there is a potential downfall to this idea that must be understood. Innovation would undoubtedly suffer if technological capabilities were limited in the design process. This is a cost worth enduring. Innovation and the evolution of modern technology obviously should never be completely abandoned, as they protect the ability of American businesses to continue to thrive in an ever-changing landscape. However, technological engineers should not be encouraged to prioritize the success of a potential business client over the privacy rights of individuals as a whole. It is difficult for companies to look the other way regarding invasive technologies when

[9] Don Norman, The Design of Everyday Things (Basic Books, 1988).

engineers are making such equipment available. The competition between data collection companies will only continue to become more intense, meaning the time is now for law to step in and provide some guidance on the development of this equipment.

Regardless of the specific approach that the United States decides to take regarding the protection of privacy rights, there is clearly a need for a change in the current system. Although the capitalistic nature of the United States will always side with preserving the ability of American companies to flourish, recent data breaches across the country and the world express a strong demand for change. The pressing problem is that companies are collecting and distributing sensitive data from their consumers, without consumers even knowing this information is out in the internet world. This affects redressability on both sides and this fact has already been exemplified by the data breaches that have occurred around the world recently. Harm suffered from invasion of privacy can be just as severe as any other harm, if not worse. Yet in many instances, the law prevents data subjects, whose privacy has undoubtedly been invaded, from seeking a sufficient legal remedy. The United States must follow the footsteps of the GDPR in some fashion; even if the FTC would like to preserve the sectoral law system, there must be changes made to it. No matter the specifics, there needs to be a shift towards protecting the privacy rights of the consumer and the nature of the data being collected, instead of protecting the commercial interests of American companies at the expense of privacy.