Introduction to Consumer Privacy

As a global leader, the U.S. should be exemplary to the world outside, especially on law as important and critical to our everyday society as consumer privacy. Unfortunately, privacy law was never a priority in this country, until Warren and Brandeis changed that with their article "The Right to Privacy."[1] Although this groundbreaking article changed how American's thought about privacy, it never allowed for cohesive law to rise, leaving the nation vulnerable, even more so in the technological age.

Presently, the United States has only been subject to sectoral doctrine that dictates the states individually to create and enforce its own laws, rather than a conducive federal system that regulates on a national scale. These laws usually include some form of "notice-and-choice," which originated from the Fair Information Practices Principles (FIPPs) which were developed in 1973 from the federal Department of Housing, Education and Welfare.[2] One of the exceptions to this was the California Consumer Privacy Act (CCPA),[3] a clear example of serious consumer privacy principles and protection from data controllers who until recently had extreme leniency during collection and use of consumer data. Although California has made great progress, this still leaves the majority of consumers in the U.S. powerless against data controllers and without the ability to enter federal courts when privacy is breached. Without uniformity on a national scale, most U.S. consumers will be left without the ability to protect

[1] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (2018)

[2] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (2018)

[3] CCPA, California Consumer Privacy Act of 2018, https://iapp.org/resources/article/california-consumer-privacy-act-of-2018/ (Oct 22, 2018).

themselves from data controllers unfair "consent" policies that in actuality give little to no protection. With every passing technological innovation also comes the constant diminution of consumer privacy. To combat the issue of consumer privacy we must first, enhance consumer privacy by implementing an all encompassing federal law that has innovative privacy measures that mirror the GDPR (and CCPA), including an extensive definition section[4], the right to be informed[5], right to deletion (be forgotten)[6], data minimization,[7] and penalties/punishment for data controllers who breach.[8] Second, to fill the gaps left by the GDPR, create privacy policies that cohesively explain consumer privacy options with inherent privacy designs[9] to allow for simple comprehension by consumers. With these robust changes in privacy law, national harmonization of consumer privacy would occur, and global harmonization could become a reality for the future.

[4] Art. 4 GDPR — Definitions, General Data Protection Regulation (GDPR), (Oct 26, 2018).

[5] Art. 12 GDPR — Transparent information, communication and modalities for the exercise of the rights of the data subject, General Data Protection Regulation (GDPR), (Oct 29, 2018).

[6] Art. 17 GDPR —Right to erasure ('right to be forgotten'), General Data Protection Regulation (GDPR), (Oct 24, 2018).

[7] Art. 5 GDPR — Principles relating to processing of personal data, General Data Protection Regulation (GDPR), (Oct 26, 2018).

[8] Art. 84 GDPR — Penalties, General Data Protection Regulation (GDPR), (Oct 26, 2018).

[9] Art. 25 GDPR — Data protection by design and by default, General Data Protection Regulation (GDPR), (Oct 26, 2018).

At Present: Consumer Privacy as It Is

At this point what we have generally is a "notice-and-choice" regime in the United States.[10] "Notice-and-choice" has a basic format, consumers are given notice (usually in a preposterously long privacy policy) about how data controllers will use and store their data, and then the consumer can either "consent" and use the site or decide to go elsewhere. However, this privacy regime is inadequate in a number of ways, some of which are: lack of consumer protection, near-to-no regulation for data controllers, and although the name states 'choice,' there is a significant lack thereof for consumers. What may have been an adequate way to regulate data controllers at one point in time, has lost any to all its power at present. Online users of the early internet days cannot compare with how extensive online use and information is now, and consumer concerns about online privacy has become a legitimate interest for today's consumers.[11] Data is being distributed by people constantly and fluidly, one click of consent does not cover all the information that will be taken subsequent to the 'click.'

Problems with this privacy regime begin as soon as a consumer visits a website. They are generally given a privacy policy and will not take the time to read the fine print involved with using the site, which is reasonable since no one has time to read the long policies that data controllers create. Then after one click of consent the data controllers now have the ability to collect and store data. What is even more troubling is that the privacy policies will not explain exactly what the collection entails (if it's limited to what the website needs to perform the task at hand) or if it will continue to collect ones

[10] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (2018)

[11] Sheila F. Anthony, *The Case for Standardization of Privacy Policy Formats* (July 1, 2001)

content without limitations. Even if the policy by chance states that data is limited, consumers will not know how much information has actually been or will be collected and the contradictory language of policies only inhibits this lack of knowledge[12]. The policies are just inadequate[13], since they don't give consumers the tools to understand what data controllers are actually doing.[14] They in most cases, only create policies in order to comply with the FTC[15] (and yet do not fulfill half the obligations they should), perpetuating this lack of strength in consumer privacy policy. Additionally, policies can be changed rather frequently, without any notice to consumers, only adding to the inadequacy of 'consent' in this regime.[16] With all the flaws that come with "notice-and-choice," better options exist in order to properly protect consumers and it begins with a more robust privacy regime, such as the GDPR and CCPA.

For the Future: Consumer Privacy as it Should Be

In order to reach better data protection, we must fill the holes that the sectoral privacy regimes in the United States have allowed. With each data controller creating its own privacy policies, it allows for them (data controllers) to greatly undermine basic privacy rights and abuse the few checks that are present in the U.S. In order to combat this, a more cohesive and all-encompassing law must be set in place. What can help

[12] Sheila F. Anthony, *The Case for Standardization of Privacy Policy Formats* (July 1, 2001)

[13] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (2018)

[14] Lisa Sotto, *Notice and Choice Paradigm in the US: Shifting the Focus*; Data Protection Law and Policy (2010).

[15] *The Status of Online Privacy*, Federal Trade Commission (2013), https://www.ftc.gov/public-statements/2000/06/status-online-privacy (Oct 22, 2018).

[16] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (2018)

create a more fluid transition is the fact that there are robust models already in place that the U.S. can use to improve and innovate its consumer privacy, the GDPR (General Data Protection Regulation) and California Consumer Privacy Act (CCPA).

The GDPR is an act that works across the EU (European Union) providing guidelines and consumer privacy in a real and effective way. Unlike laws that are territorial, the GDPR protects any citizen that belongs to the EU regardless of where their data is processed and does not need legislation in order to be enforced. It is a consent-based regime, however it is effective due to its vigorous protection of consumers. Also, unlike many privacy regimes, the GDPR clearly creates guideline for data controllers, which in turn creates better experiences and protection for consumers. Some of these include: detailed definitions, right to be informed, right to be forgotten, data minimization, and penalties for those who breach. Alongside the GDPR, derived heavily from it, comes a second source to aid in the creation of a new privacy regime, the California Consumer Privacy Act (CCPA). Another robust consent regime, it takes many of its main elements from the GDPR, however it pays special attention to penalties. For these reasons, the GDPR with help from the CCPA are models in which the U.S. should take great consideration when forming its own nation wide consumer privacy law. Some of the key elements provided by the GDPR and CCPA follow and would be crucial in creating the United States consumer privacy law.

The GDPR provides an extensive list of definitions in which its users can reference to see what certain words used within the regulation mean. This feature of the GDPR is one of the most important. It is not only useful in providing clarity for articles that need further explanation, but also creates a more user friendly act. Just because a

consumer is not familiar with a certain word, for example 'processing' would not affect a consumers' understanding of an article if provided a definitions section. They can look to the definitions section and learn about words and phrases that are central to the GDPR, without feeling they have missed crucial parts due to lack of understanding. These definitions also play a role in creating better understanding for data controllers. One example is providing a definition for pseudonymisation. "'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."[17] With this clear definition, data controllers can now easily understand what it is the act is requiring them to do in order to comply with pseudonymisation. Without such clear definitions, compliance would fall short of what was expected. This demonstrates the importance of definitions for consumers and data controllers alike.

Next would be the "Right to be Informed."[18] The GDPR provides extensive articles to protect consumers by forcing data controllers to 'inform' them about what is happening with consumers' own information once they visit a website. It compels data controllers to tell consumers what information has been collected and used by each site. This allows consumers to understand what and why data controllers are collecting what they are. It creates a transparency that most consumers have never seen before on

[17] Art. 4 GDPR — Definitions, General Data Protection Regulation (GDPR), (Oct 26, 2018).

[18] Art. 12 GDPR — Transparent information, communication and modalities for the exercise of the rights of the data subject, General Data Protection Regulation (GDPR), (Oct 29, 2018).

online spaces. This also helps create platforms that are more user friendly, while also keeping data controllers accountable for the information they collect. If not, the amount of information could be collected indefinitely. This "right to be informed" creates a limit in which data controllers must tailor their collection or risk loss of consumers due to absurd data collection. This also includes informing about duration of storage in accordance with consumer data. With restrictions on storage of data, a concern of many consumers, knowing how and what is being stored significantly alters the power struggle between consumers and data controllers, creating a more even balance.

Following would be the "Right to be forgotten." "The correspondingly-named rule primarily regulates erasure obligations. According to this, personal data must be erased immediately where the data are no longer needed for their original processing purpose, or the data subject has withdrawn his consent and there is no other legal ground for processing…".[19] This concept comes from a famous case, Google Spain SL v. Mario Costeja González (2014).[20] The case began from the plaintiff googling himself and finding his auction page from ten years prior when he was in debt. Plaintiff felt he had a "right to be forgotten" since this information no longer reflected who he was. After being allowed erasure, the concept was then adopted as a crucial element of the GDPR.

This element is important because with it comes great consumer power and protection. It is all based off what the consumer wants online or not. Consent can be given by a consumer, but it does not create consent forever, which is usually the case at

[19] Art. 17 GDPR —Right to erasure ('right to be forgotten'), General Data Protection Regulation (GDPR), (Oct 24, 2018).

[20] Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014)., 128 Harv. L. Rev. 735

present. Here, consumers have the ability to rescind their consent in order to amend or erase information online. This creates one of the greatest channels of trust between consumers and data controllers. If consumers do not feel limited or betrayed by information they have online and have the ability to amend or erase it, consumers will be more open and trustworthy to data controllers. Also as the GDPR states, if the data is no longer being used, they are obligated to delete it. With more and more security breaches, the knowledge that erasures are mandatory allows consumers more ease when it comes to their data. This also allows data controllers to no longer be held responsible for older data that is no longer relevant if they are performing periodic erasures.

Data minimization is simple, when consumers use a website, the site will only use information from the user that is adequate and limited to what is necessary for the function of the website.[21] It will not collect data outside of the functions it was made to do, therefore when visiting sites consumers know data being collected is relevant to the functionality. Data collection right now is near infinite. This creates an excess of data being collected from consumers purely for the benefit of the data controllers. This cannot be tolerated and demonstrates why data minimization is so important for consumer privacy.

Last are penalties (and accountability) for data controllers who breach the laws. The U.S. makes redress from breaches of privacy extremely difficult to achieve and usually leaves consumers going through laws unrelated to privacy in order to amend harm.[22] The GDPR and CCPA both address this issue and have specifically included

[21] Art. 5 GDPR — Principles relating to processing of personal data, General Data Protection Regulation (GDPR), (Oct 24, 2018).

[22] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (2018)

penalties into their articles. In the GDPR it states “fines must be effective, proportionate and dissuasive for each individual case. For the decision of whether and what level of penalty can be assessed, the authorities have a statutory catalogue of criteria which it must consider for their decision.”[23] By enforcing penalties, data controllers are skeptical when it comes to breaching. This is a deterrent to those who otherwise may not take the laws seriously. On the other hand, for smaller data controllers that do not have such deep pockets it looks at each case individually, therefore even if there is a breach due to lack of funds rather than malintent, they could be assessed accordingly.

The CCPA goes into even further detail explaining the amount that can be recovered for monetary damages, as well as injunctive or declaratory relief. This allows for consumers to feel they will actually receive some justice if a breach occurs. Without the assumption that perpetrators will be punished for breaches, the consumers cannot believe that they are being truly protected. This also provides clarity for data controllers on what they may owe consumers who's information they do not adequately protect.

One concept covered in the GDPR, but not to the extent needed is privacy by design. Although it does brush upon the topic, the GDPR does not fully articulate its importance for consumer privacy. This is arguably one of the most important aspects which must become a central element of U.S. consumer privacy. “The term “Privacy by Design” means nothing more than “data protection through technology design.”[24]

---

[23] Art. 82 GDPR — Right to compensation and liability, General Data Protection Regulation (GDPR), (Oct 24, 2018).

[24] Art. 25 GDPR – Data protection by design and by default, General Data Protection Regulation (GDPR), (Oct 24, 2018).

Simply put, websites are created to process in a way that creates the most secure code for processing information in a consumer friendly manner.

When visiting a website, if it is created with privacy as a core function, it will create a platform that can be easily understood by consumers. For example, when visiting a website as soon as it loads up, a short summary of privacy options appear. In the options we have: 1) the ability to allow data to be used for this site in accordance with website function (better consumer experience) 2) data used for this site, plus allowed to be given/sold to 3rd parties, or 3) we do not want our data to be taken by the site at all. With clear options and a summary of what they mean, not in fine print but displayed clearly, creates a completely different online experience. No longer are consumers under the impression that they must consent, but rather are given real time options in which to manage their own information. This being hardwired into the design of a website completely redefines how online users understand online privacy. Keeping this concept at the core of a websites code is not only helpful for consumers, but allows for trust to be created between consumer and data controller. With this in mind, consumers would feel more comfortable sharing more frequently, while also allowing for data controllers to more simply manage information. Once consumers make the decision based on clear identifiers on a consent page, there can be a clear "meeting of the minds" that never occurred before with lengthy policies. With these elements in place, in addition to those within the GDPR and CCPA, online platforms can become consumer friendly, while also creating clear guidelines for data controllers. This could lead to true national harmonization.

Ultimate Goal: National harmonization (eventually global)

In order to reach national privacy harmonization, it is crucial the United States adopts a vigorous federal law providing clarity, protection, and accessibility to consumers and data controllers alike. By implementing main principles of the GDPR and CCPA, while also tying in elements of privacy by design, there can finally be cohesive consumer privacy law. Even if it begins slowly, overtime this method can work to create a better online platform for all. Also by mirroring policies by the GDPR the U.S. is taking major steps to harmonize privacy law between itself and the European Union. This would send a clear message to consumers about the importance of their privacy, while demonstrating to data controllers that their abuse on lenient laws has gone to far. In summation, privacy law would be changed for the better, enabling consumers to take back the power of their own online information.