Docket No. 180821780– 8780–01
Department of Commerce
National Telecommunications and Information Administration
Request for Comments

Data Protection through Privacy by Design

Stephanie Saraiva

1. Introduction to Privacy

In 1890, future Supreme Court Justice Louis Brandeis and attorney Samuel Warren published an article in the Harvard Law Review, "The Right to Privacy," which argued for the legal right to "be let alone." The article was prompted by a new technology called the instantaneous photograph, which made it possible for anyone walking down the street to find their image in the newspaper the next day. [1]Today, however, this distinction has eroded, thanks to the rapid advance of digital technologies and the lack of data protections systems incorporated in the design of companies. [2]Brandeis and Warren argued for the right to be let alone, which is a right to retreat from the world and retreat in the privacy of our homes. There is a distinct difference from being observed, which can accompany any act made in public, versus being identified, a separate and more intrusive act. [3]We consent to be observed constantly but we rarely consent to be identified.[4]

---

[1] Burt, A., & Geer, D. (2017, October 05). The End of Privacy. https://www.nytimes.com/2017/10/05/opinion/privacy-rights-security-breaches.html
[2] Id.
[3] Id.
[4] Id.

2. Failure of Consumer Privacy Bill of Rights

The argument Brandeis and Warren proposed many years ago is still the basis for the way we approach our rights to privacy today. In 2012, President Obama introduced the Consumer Privacy Bill of Rights, which intended to give American's the ability to exercise control over what personal details companies collected from them, how the data was used, and gave consumers the right to see and correct records that companies hold about them. [5]The Obama administration called on Congress to enact the Consumer Privacy Bill of Rights which was supposed to apply to industries not already covered by sectoral privacy laws. These industries included data brokers, companies that collect details on an individual's likes, leisure pursuits, shopping habits, financial status, health interests and more. [6] The bill proposed privacy as a basic American right, however the effort was unsuccessful. The bill was not only incomplete but produced very few data controls for consumers. The bill was dependent on the autonomy of companies and left it up to industries to decide what to do, leaving no incentive for companies to compromise.

3. General Data Protection Regulation and Article 25

During the same year, the council of the European Union proposed the General Data Protection Regulation(GDPR). The proposal aimed for the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

---

[5] Singer, N. (2017, December 21). Why a Push for Online Privacy Is Bogged Down in Washington. https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html

[6] Id.

penalties, and the free movement of such data, which is intended to replace the 2008 Data Protection Framework Decision. [7]The aim of the GDPR was to reinforce data protection rights of individuals, facilitate the free flow of personal data in the digital single market and reduce administrative burden. [8]

Among the requirements laid down in the reformed rules is the adoption of Privacy by Design. Article 25 of the GDPR focuses on the implementation of privacy measures into the design of the process. Privacy by Design is the approach focused on maximizing privacy and data protection by embedding safeguards across the design and development of products, services or processes by taking privacy and data protection considerations into account from the outset and throughout their whole lifecycle, rather than as a remedial afterthought.[9] Safeguards should be built into the core of the products, services or processes and treated as a default setting for not only technologies, but also operation systems, work processes, management structures, physical spaces and networked infrastructures.[10] Companies engage in Privacy by Design when they promote consumer privacy throughout their organizations and at every stage of the development of their products and services.[11]

4. The concept of Privacy by Design

The concept of Privacy by Design was developed back in the 1990's by Ann Cavoukian, in order to address the ever-growing systemic effects of wide spread personally identifiable information. Cavoukian lays out seven foundational principles.

---

[7] Belgium, Council of the European Union. (2012.). *Proposal for A General Data Protection Regulation*.
[8] Id.
9. European Union Agency for Network and Information Security (ENISA). (2014, December).
[10] Davies S, 'Why privacy by design is the next crucial step for privacy protection' [2010], http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf
[11] Id.

First, The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen.[12] Second, Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default. [13] Third, Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. Privacy is integral to the system, without diminishing functionality.[14] Fourth, Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. [15]Fifth, Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to end.[16] Sixth, Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. [17] Last, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. [18]

---

[12] Cavoukian, A. The Seven Foundational Principles.https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/

[13] Id.
[14] Id.
[15] Id.
[16] Id.
[17] Id.
[18] Id.

5. Issues with Cavoukian's Seven Foundational Principles

While these seven foundation principles by Cavoukain may seem promising, they do not come up with any mechanisms in order integrate privacy in the development process of the system. Several researchers and data protection commissioners have published guidelines on how Privacy by Design could be understood. However, many system developers are not familiar with privacy principles or technologies that implement them. Their work usually focuses on realizing functional requirements, where other demands such privacy or security fall short as a result. Also, the developing tools provided by software companies hardly considers privacy principles. It is no easy to overcome those shortcomings because there are conceptual difficulties in guaranteeing privacy properties in systems such as adopting to system change requirements. [19]Still, the degree of implementation of privacy principles and privacy requirements in the design process should be considerably increased, no matter whether this will be demanded by law or not.

6. What is "Design" in Privacy by Design?

To design is to create a plan for the construction of something.[20] In systems development, it is essential to come up with a suitable design structure before implementation.[21] This also means drawing out a suitable plan for how the system will be created from the onset. Design is a core stage of the life cycle of systems. Specified system requirements and analysis of design goals are inputs that are used in the design of systems.[22] In the same way that functionality and

---

[19] European Union Agency for Network and Information Security (ENISA). (2014, December*). Privacy and Data Protection by Design*.
[20] Springer.(2012).Jeroen van Rest, Daniel Boonstra, Maarten Everts, Martin van Rijn, and Ron van Paassen. *Designing privacy-by-design*.
[21] Id.
[22] Id.

efficiency are designed into the structure, privacy features should be planned and designed into the system early on, instead of implemented in later stages of development, or sometimes not even at all. Basically, privacy features should be engineered into the design of the system.

7. Engineering Privacy into the Design

Article 25 of the GDPR states" *the controller (the person processing the information) shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."*[23]

Engineering privacy into the design of a system tends to minimize the risk of privacy breaches by minimizing trust in data collectors and processors handling sensitive data properly. [24]Further privacy design strategies can be applied to increase the integrity and transparency of systems once sensitive data flows to data collectors and processors. Data minimization refers to not collecting certain data inputs, i.e., if not necessary for achieving the desired functionality of the system, data should not be collected in the first place.[25] By ensuring that no unnecessary data is collected, the possible privacy impact of a system is limited. Engineers may reasonably implement data minimization in many different ways such as, limiting the capture and storage of

---

[23] Art. 25 GDPR – Data protection by design and by default. https://gdpr-info.eu/art-25-gdpr/
[24] Gurses, S., & Troncoso, C. Engineering Privacy By Design Reloaded. Retrieved from https://iapp.org/media/pdf/resource_center/Engineering-PbD-Reloaded.pdf.
[25] id.

data in the system, constraining the flow of information to third parties, limiting the amount of entities where data is stored or processes, limiting the inferences that can be made my linking data, or minimizing the retention of data in the system.[26] Privacy-preserving systems typically aim to protect privacy by combining these principles. A data minimization example may be the use of pseudonymization (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorized can read them)[27].There will always be a balancing test when implementing privacy systems into the design. Designers and engineers should take into account the costs of implementation of any measures, the nature, scope, context and purposes of processing and the risks that processing poses to the rights and freedoms of individuals.[28]

8. The GDPR and CalOPPA

Consent as stated in the GDPR must be explicit, and a request for consent to a data subject must be clearly stated to allow for lawful processing.[29] The data subject should also be able to withdraw consent to the processing of the data subject's personal data at any given time. [30]The GDPR clarifies that if a particular processing has different purposes, consent should be given by the data subject for each individual purpose. Notification should be clear and in plain language.[31]

---

[26] Id.
[27] Art. 25 GDPR – Data protection by design and by default. https://gdpr-info.eu/art-25-gdpr/
[28] Id.
[29] Consent GDPR https://gdpr-info.eu/issues/consent/
[30] Id.
[31] Id.

A notification cannot be hidden among other information. Notification of data breach should also be in clear and plain language.[32] Recital 39 of the regulation states that *"In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language".*[33]

Similar to the clear and plain language standard in the GDPR, the California Online Privacy Protection act also requires a company's privacy policy to be conspicuous.

CalOPPA requires the website to feature a conspicuous privacy policy stating exactly what information is collected and with whom it is shared; it also requires the operator of the website or online service to comply with the site's privacy policy. [34]Those who fail to do so are at risk of civil litigation under the state's Unfair Competition Law. [35]The operator of a commercial website or online service must conspicuously post a privacy policy on its website.

According to CalOPPA, websites can conspicuously post a privacy policy in a variety of different ways. First, the privacy policy is shown on the website's homepage. [36]Second, a link – via an icon that contains the word "privacy" – appears on the homepage and directly takes consumers to the privacy policy. In this instance, the icon must be in a color different from the homepage's background. [37]Third, the privacy policy is linked to the homepage via a hypertext link that contains the word "privacy," is written in capital letters equal to or greater in size than

---

[32] Id.
[33] Recital 39 GDPR. https://gdpr-info.eu/recitals/no-39/
[34] Education Foundation. (2015, July). https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/
[35] Id.
[36] Id.
[37] Id.

the surrounding text; is displayed in a type, font or color that contrasts with the surrounding text of the same size; or is otherwise distinguishable from surrounding text on the homepage.[38]

9. The GDPR and CCPA

Similar to Article 25 of the GDPR, the California Consumer Privacy Act also regulates what kind of information business may collect from consumers. Section 1798.100(b) of the act states *"A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."* [39] Similarly, Article 25 states the controller, the person processing the information, should implement data protection principles, such as data minimization. CCPA is saying that businesses must use data for a particular purpose and must state what they are using the data for. Businesses are not permitted to take data and then use it for other purposes not stated. While the GDPR was created to protect citizens of the EU, its impact extents much farther. The CCPA is an outcome of the GDPR's reaching influence, shifting government priorities and making them more willing to protect individual privacy. CCPA will serve to protect California consumer rights and encourage stronger privacy and greater transparency overall. It will give consumers ownership, control, and security over their personal information – and consumers will have the ability to

[38] Id.

[39] California Consumer Protection Act. https://iapp.org/resources/article/california-consumer-privacy-act-of-2018/

request that any business disclose (and delete) the personal information that it collects, and request that their data not be sold to third parties. [40]

These data protections give Californians the right to: know what personal information is being collected, access the personal information that is collected, and request it be deleted, know whether their personal information is being shared, and if so, with whom, opt-out of the sale of their personal information, have equal service and price, whether or not they choose to exercise their privacy rights.[41] Unlike the Consumer Privacy Bill of Rights, CCPA is a comprehensive data protection regulation that can be used an example for other state and federal laws moving forward in order to force companies to be accountable for protecting consumer data.

10. Why should Privacy by implemented into Design?

Privacy should be implemented into the design of a system or software so that companies do not have to deal with privacy problems after the fact. Companies are better equipped to take action on privacy matters than consumers are. Imbedding privacy processes to begin with in most cases would be cheaper. It is easier for a company to design measures in order to prevent problems such as data breaches, than to go through the expense of going through a law suits after a data breach.

For instance, earlier this year, Facebook had a security breach that affected over 50 million users. 50 million users had their personal identifiable information exposed, which includes name, email address, recovery email accounts, telephone numbers, birthdates,

---

[40] California Consumer Privacy Act (CCPA) vs. GDPR. (2018, November 05). https://www.varonis.com/blog/ccpa-vs-gdpr/

[41] Id.

passwords and security question answers. [42]A class action suit was filed in California on behalf of the 50 million users, and the complaint alleges that Facebook's privacy policies are grossly inadequate and their lack of security measures have made users more susceptible to identify theft. [43]

Facebook is not the only company that has experienced data breaches, in fact this is an extremely common occurrence. As the spread of data and personally identifiable information becomes even more widespread in today's world, data breaches will continue to be a common occurrence unless companies step in and take proactive measures. Unfortunately, most companies do not care enough about consumer's privacy. Therefore, companies put privacy measures on the back burner and put their focus on design for functionality and efficiency, rather than privacy.

Unlike the Consumer Privacy Bill of Rights, the GDPR does not give companies the choice to comply with the law or not. Therefore, companies that do business with countries in the European Union must comply with the GDPR and implement reasonable data protection measures. Even when companies care about consumer's privacy, if they do not design the structure of the company with privacy in mind and engineer privacy into it, there would be difficulties in preventing data breaches. Many companies can only handle data protections problems as a reactive measure, instead of a proactive one. Furthermore, companies have more knowledge and are in a better position to understand privacy concerns, rather than the consumer.

---

[42] Fabio, M. (2018, October 01). Facebook Faces Class Action Over Security Breach That Affected 50 Million Users. https://www.forbes.com/sites/michellefabio/2018/09/30/facebook-faces-class-action-over-security-breach-that-affected-50-million-users/#53fb24f97b6c

[43] Id.

Implementing data privacy by design, at a minimum, can insure that only personal data necessary for a specific purpose is collected, data that is no longer needed would be deleted, and people can opt in or opt out of any collection, storage, processing, or deletion of their personal data.

11. Recommendations

Legislators must promote the importance of privacy and data protection. In making laws, on the state and federal level, legislators should look to the GDPR, especially Article 25 that deals with Privacy by Design. Legislators should also look to already enacted laws such as CalOPPA and soon to be enacted CCPA, which are two comprehensive data protection laws in the United States that force companies and business into compliance, unlike the Consumer Privacy Bill of Rights. Finally, engineering in privacy should be further investigated with respect to mechanisms that would help engineers and designers to implement data protection principles into the design of the system in order to be proactive and preventive instead of reactive.