NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

Privacy in Europe Explained for Americans: Part II

By Donna Gallaher
CISSP, C|CISO,
CIPP/E, CIPM, FIP

PRIVACY IN EUROPE EXPLAINED FOR AMERICANS: PART II

In Part I, we discussed the history of data privacy in Europe and the US while also introducing the OECD Guidelines as the universal standard for data privacy. However, implementing this change is easier said than done. As Europe learned after World War II, uniting a few dozen independent states into a single framework is a major challenge, analogous to what will need to happen in the United States.

Regulated companies in industries such as healthcare and financial services usually manage multiple state breach notification requirements by adopting the most restrictive state as the standard or through limiting service by either geography or solution functionality. Up to this point, most B2C businesses have experienced limited regulation. As a result, the California Consumer Privacy Act (CCPA) was a shock to the industry. This bellwether legislation is still being amended to ease the blow to businesses when it finally takes effect on January 1, 2020. Once a single federal standard is adopted, companies will not have anywhere to hide. They must comply or suffer the consequences.

For this reason, it is critical that we balance a fundamental right to privacy against the burdens placed on businesses, or the economy may suffer. The legislative considerations include ethics, economic impact, implementation, and enforcement challenges as discussed in greater detail in this whitepaper.

ETHICS AND DATA PRIVACY

Americans use technology when making even the most basic decisions. A user might expect an objective answer when asking Siri where to go for dinner or Waze to determine the fastest way downtown. Those targeted, subjective responses may cause limited harm, if any. However, a time may arrive when we become so used to answers fed to us upon request that we eventually lose our ability to discern truth from spin. The result? Deferring moral and ethical decisions to an Artificial Intelligence paid for by an unknown entity with an unknown agenda, and those decisions may cause harm.

Our example of the married couple in Part I of this whitepaper touched upon the accessibility of their profile data to divorce attorneys and dating websites. As we saw with the husband and wife, ads targeted to consumers can appear closely related to their profile data. In other cases, consumers may not know who is interested in their profile information or why they have been targeted, and the AI that provides answers might not reveal if the provided response is objective or based on a targeted advertisement.

To further illustrate the point, suppose the pregnant teenager we referenced in Part I began asking Siri about abortion or voting recommendations. Or, what if an elderly

person asks about new medical treatments or euthanasia and expects to receive objective answers? The user pays for both the internet service and device, and the AI knows "everything" about the user including age and religious affiliation. It should base its content delivery decisions off "your profile," right? But without a universal consensus about what "your profile" means, it becomes a subjective term.

Trusting the AI to deliver objective information becomes less certain when profile information is sold based on market value. What if parents wish to raise their children with different values than those exhibited in popular movies and television shows? What if insurance companies prefer options that limit expense over unproven life preserving options? Without transparency in the AI's algorithm, there is no guarantee that the options presented are truly optimized for the consumer—and it's unlikely that a user would detect manipulation. The answers provided by the AI and the information the consumer should be entitled to know about how the AI makes its recommendations will require consensus not just from a compliance perspective but from an ethical perspective. Otherwise, people may become nothing but data points associated with a credit rating or market value rather than free individuals. Regardless of political affiliation, no one wants that freedom taken away.

In the United States, we are quick to assume that consumers will surrender all privacy rights for a free app. Up to this point, consumers have had little choice. However, the idea of unrestricted and broad consent to the surrender of any and all information that could be useful to a company at some point in the future would not exist if Americans had the same privacy rights as in other parts of the world. But that's changing with more consumer awareness and negative publicity about data privacy issues that harm people. In the September 2018 Senate hearings sponsored by Sen. John Thune (R-South Dakota), even the industry leaders receiving the brunt of privacy criticism from the EU acknowledged that privacy regulation in the US was inevitable. The challenge is how and when to start.

PRIVACY VERSUS ECONOMY BALANCE

When introduced to the OECD Privacy Principles, most consumers agree conceptually with these fundamental principles. So, what's the resistance? Regulation always comes at a cost.

A trade-off exists between the regulation of personal privacy and—you guessed it—the economic impact. There is a reason why the United States produces the highest percentage of the world's GDP and the EU's economic status is slipping. Over the past two years, the United States government has been working to reduce the amount of regulation due to its stifling effect on the economy. As a result, the US is enjoying enormous prosperity both in GDP growth and record low unemployment numbers.

Although Europe has a 70-year head start on addressing privacy as a human right, they are experiencing implementation challenges and associated costs. The GDPR calls for certifications and marks to certify the adequacy of as yet uncreated privacy programs, and the harmonizing of penalties across the Data Protection Authority has not been completed. The Data Protection Authorities will surely have challenges meeting the increased workload of assistance requests from both businesses and individuals. Although GDPR requires member countries to provide adequate resources to operate these agencies, the money must come from somewhere. If the intention was to fund the enforcement agencies through fines, it may be some time before any funds are collected and available to use for program operations, especially for companies outside the EU.

As for data flows between the US and EU, we are at somewhat of an impasse with regard to data privacy as the European Court of Justice considers sufficiency challenges to the US-EU Privacy Shield. It doesn't look good. While some argue that GDPR presumes a privacy program is insufficient until proven adequate and that the fines may be used to siphon revenues from the US to the EU, others would argue that the European Data Protection Authorities have shown great restraint in imposing fines and only penalizing offenders for the most egregious violations. Further complicating the equilibrium is how GDPR becomes politically involved in the debate regarding trade agreements, tariffs, and offsetting penalties between countries.

Any new US regulation will place a resource burden on targeted companies, on the government to monitor and enforce, and on the economy. The passage of GDPR exposed previously unregulated B2C companies within its territorial and material scope to a whole new world of regulation, sending a shock wave across the United States. Companies unwilling or unable to redesign their business model are attempting to achieve compliance through checklists, by ceasing operations in the EU, or by ceasing the data processing of EU data subjects. However, B2C companies are only now beginning to understand the far-reaching impact of GDPR in their supply chain. Without adequate Third-Party Oversight (TPO) programs, these companies may still find themselves in the position of a data controller with inadequate controls on their data processors—subject to fines, class action lawsuits, reputational damage, and legal costs.

GDPR provides for several methods of demonstrating policy compliance including the adoption of standard contract clauses published by the European Data Protection Board between parties, custom contract terms reviewed and approved by the Data Protection Authority, or Binding Corporate Rules (BCRs) used within a multinational organization. Again, if your business model is incompatible with the EU view of personal data privacy, compliance will be nearly impossible to attain.

As Congress debates the new equilibrium between privacy and free expression, careful consideration should be made about how the economic impact of federal regulation may

offset the negative impact of state regulations. Many states are already considering their own regulations in the wake of California's privacy law, and we know from data breach notification laws that 50 state regulations are more burdensome on industry compliance than one federal regulation. Pre-empting this catastrophe is advantageous to business.

To satisfy the European regulators from an accountability perspective, the Federal Trade Commission (FTC) will most likely become the US regulatory federal entity responsible for privacy law enforcement. To serve this function, the FTC will also likely need additional income from new taxes or fines to enforce these new privacy laws (including GDPR). With the FTC acting as the privacy enforcer, the defense of privacy infractions will be left to individual companies. Even if the little guy wins, it could mean bankruptcy for the company and its officers.

Although the issue litigated was information security rather than privacy compliance, the LabMD case highlights the disadvantage that a small company has when battling the federal government. Michael Daugherty, the former CEO of LabMD, ultimately prevailed in his case against the FTC in June 2018—but only after losing his business and life savings.

With so many companies gathering, buying, selling, churning, and interpreting data, privacy regulation can easily become so complicated that it becomes impossible to comply and instead play out with never-ending litigation costs. Because multiple entities can buy and sell the same privacy data elements, attribution of source data may be impossible. Although large companies may have the resources to set up comprehensive privacy programs, smaller and less visible companies may leak personal privacy information willingly or unwillingly. Once it's out, it's out.

Despite all these issues, there are specific ways we can improve privacy regulation in the US. Its inevitability doesn't need to compromise business ethics or hurt the economy.

IMPROVEMENTS NEEDED IN US PRIVACY REGULATION

Both GDPR and the CCPA discuss in great detail the requirements for the transmission of privacy information by a data controller, but they fail to address the **receipt** of consumer information. This may be the key to simplifying accountability issues in the United States. Strategies which decrease the value of personal data will have a bigger impact than those that focus on the processing of data.

To illustrate this subtlety, note that GDPR focuses on the relationship between a Controller (company) and the data subject (consumer), allowing the Controller to obtain data either by consent of the data subject or from another source for a legitimate business requirement. Processors are obliged to assist Controllers with consent changes but are very limited in their responsibilities to the data subject/consumer.

Furthermore, the Controller is only required to pass along the request for opt-out, deletion, correction of the information, etc. to the Processor. If there are any questions or problems with the use of personal data, the data subject/consumer only needs to contact the Controller and the Controller will coordinate with any Processors involved.

Also note that because of the respect for personal privacy as a fundamental right in Europe, a large market for **legally** buying and selling personal data in the EU does not exist as in the US. In the EU, the acquirer and user of privacy data is likely the same entity (the Controller). As a result, rules governing the relationships between the data subject, Controller, and Processor may be adequate in Europe but unmanageable in the US because the user has no control over the source of the data.

In the US, data aggregators that buy and sell consumer data are technically Controllers, but consumers don't know who these companies are or how to find them. Consumers only know what ads they received and the Controllers that delivered those ads may have limited authority to effect change over other Controllers. Under GDPR, those Controllers should cease doing business with those "Aggregator-Controllers." However, they will still be allowed to sell the data to another company and the consumer will have no recourse.

Consumer personal data is considered a commodity in the US, and the companies that buy and sell their data have no established relationship with the consumer. US-based Controllers wishing to improve and tailor customer experiences can legally buy and sell whatever data they desire to gather on their target customers without any consent, so US privacy regulations should focus on **how data is acquired** rather than **how it is used once it is received,** a distinction unique to the US. Otherwise, personal data obtained through aggregators can be sold over and over again with the consumer never having the opportunity to consent, object, or correct data sold about them.

The basis of a universally acceptable US privacy regulation works on the premise that a personal data record or profile information that cannot be legally used has a diminished value. In other words, a company is less likely to pay for personal data that it cannot use legally. Treating the **receipt** of privacy information from an undocumented source like the receipt of stolen property will appeal to global regulators. Unless a company can demonstrate that the source of the privacy data follows the OECD Privacy Principles and valid consent was obtained, it cannot be used and must be destroyed—and offenders may be subject to fines and lawsuits. This strategy combats the problem raised by aggregators and allows the rest of the GDPR to function as intended.

Plus, an additional benefit of this strategy is improved accountability for consumers. Customer service and sales departments rarely have any idea where the data they use originated or how a particular entry was added to the database. Getting removed from such a database is nearly impossible. Instead, the company should be able to tell a consumer who receives an ad where the data came from (company name and contact

information) and why they were targeted for the advertisement. That way, the consumer can correct the record or withdraw consent if they no longer wish to receive targeted advertisements.

Logging technology used by security teams to detect anomalies and integrity issues can easily identify all the details for changes made to an individual record. Similarly, the company will know how their targeting algorithm works, and so they should also be able to tell a consumer why they were targeted. Using this approach allows consumers to correct data at its source rather than addressing each of the thousands of companies buying and selling the data.

GO-FORWARD RECOMMENDATIONS

It seems that no ideal options exist when it comes to data privacy alignment with the EU. Regulations are burdensome on US government and business, with negative economic impact in a global economy. The best we can hope for is to proceed with the least amount of damage. To achieve a balance between privacy and free expression that suits both the EU and the US consumer, the following must happen:

- Recognize privacy as a fundamental human right, and adopt the OECD Privacy Principles.
- Recognize personal data as an asset with value, and provide a mechanism to validate that the asset was acquired legally before it can be used.
- Recognize that a single regulation is easier to comply with than multiple regulations.
- Recognize the impact of regulation enforcement on business, and include incentives for businesses to improve privacy programs and protections. This may include pooling GDPR fines with the EU and/or allocating funds received from US companies for US privacy improvement programs to prevent the targeting of US companies by foreign regulators.
- Recognize that consumers will rely on Artificial Intelligence for decisions, and advise the consumer how to obtain objective information.
- To the extent possible, synchronize DO NOT CALL / EMAIL registries to consolidate source data. This recommendation is intended to simplify managing changes to consumer consent preferences by centralizing the source data used by telemarketers and/or digital marketing companies.

While Congress debates privacy regulation, companies can take the free market approach to the problem and use the “Privacy by Design” and “Privacy by Default” (“PbD”) mantra to ensure their products and services meet the expectations of the global marketplace and proactively position themselves for any future flavor of privacy regulation.

What's your take on data privacy in the United States? What do you feel needs to be done at a national level? Share your thoughts with the NTSC by contacting us at ***info@ntsc.org***

Donna Gallaher served as a C-Level Strategic Advisor in IT and Cyber Strategy for multiple global companies for over 15 years drawing from her previous successes in engineering, solution selling, IT operations and leadership. Ms. Gallaher serves on the Board of Directors of the Technology Association of Georgia Information Security Society, Evanta CISO Southeast Governing Body and is active in the local ISSA and Cloud Security Alliance chapters. She is active in the lobby efforts to shape cyber security legislation and her recent articles have been published on the National Technology Security Coalition website. Ms. Gallaher holds CISSP, CCISO, CIPP/E, CIPM, ITIL, and FIP certifications and is a graduate of Auburn University with a Bachelor of Science in Electrical Engineering.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION