NTSC
NATIONAL TECHNOLOGY SECURITY COALITION

Privacy in Europe Explained for Americans: Part I

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

PRIVACY IN EUROPE EXPLAINED FOR AMERICANS

Although Europe represents a significant portion of the world economy, most American companies do not view privacy from a European consumer's perspective and struggle to make products and services that appeal to consumers outside the United States. Privacy is not a new concept in the US. It's just viewed differently. In both European and American culture, free expression and privacy are considered hallmarks of society. However, these concepts are inversely related and the balance is shifted on either side of the Atlantic Ocean. This balance shift between free expression and privacy will remain a point of contention until a new equilibrium is reached.

Understanding the European view of data privacy outlined in this whitepaper may move the debate forward in the United States as well as position companies for both compliance and improved global consumer acceptance by adopting universally accepted privacy design standards.

PRIVACY IN THE UNITED STATES

As early as our founding, the Bill of Rights recognized both a need for free expression and privacy as codified in the First and Fourth Amendments to the US Constitution. Congress may not create laws that abridge free expression or laws that detract from a fundamental right to the security of personal safety and property ("to be secure in their persons, houses, papers, and effects …"). Although the US Constitution and Bill of Rights places limits on what the government can and cannot do, free expression and privacy rights may not be automatically extended to private corporations or individuals.

Over the past 200 years, the balance between privacy and free expression in the private sector has been challenged and clarified as needed in cases such as Katz v. United States (1967), which introduced the concept of personal privacy related to electronic communications. Similarly, the murder of actress Rebecca Schaeffer in 1989 after a stalker discovered her home address through driver's license records led to laws such as the 1994 Driver's Privacy Protection Act and America's first anti-stalking laws.

In the late 1990s, the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Children's Online Privacy Protection Act (COPPA) all introduced new privacy regulations to the private sector in the United States—and compliance with these regulations remains an ongoing challenge for American companies. However, during the 2000s and early 2010s, the United States saw the rise of companies like Google, Amazon, Netflix, and Facebook which relied on personal data as part of their business model. The US economy enjoyed the economic growth of these companies largely because they were unencumbered by personal privacy regulations.

Few in the United States seemed interested in the ethical issues surrounding the ownership of personal data until 2012 when retail giant Target made headlines. Target used consumer profile information to predict pregnancy based on product purchases, which resulted in a teenage girl who had been concealing her pregnancy from her father receiving targeted marketing coupons from the retailer. Despite this incident and numerous high-profile data breaches that continue to this day, American consumers still favored a personalized customer experience and were mainly concerned about identity theft and financial information misuse.

However, the apathy surrounding privacy may finally be changing in America. Both the Equifax data breach and Facebook–Cambridge Analytica data scandal woke America up to the risks of the commoditization of personal data. In July 2018, California's California Consumer Privacy Act (CCPA) became the first US post-GDPR privacy legislation passed domestically—with other states following suit. Now, new federal privacy legislation is being debated in Congress to meet public demand and interest. What does this proposed legislation mean for companies that must eventually comply with it?

PRIVACY COMPLIANCE

CISOs are all too familiar with the reality that compliance does not equal security, and the same will be true for privacy compliance. In creating an information security program, many organizations address only what must be done at a minimum to achieve regulatory compliance rather than add controls to more fully minimize operational risk from given cyber threats. This "compliance checklist" approach to data privacy compliance will not satisfy European regulators because GDPR mandates "Privacy by Design and Default" and a proactive demonstration of compliance through the GDPR's "Accountability Principle."

Rather than continually struggle with compliance checklists, American companies need an understanding of EU privacy to achieve the "Privacy by Design and Default" requirement and commit to build solutions that meet the privacy expectations of a major portion of the world's consumer population. An appreciation for smart solution design which incorporates Privacy by Design and Default will better position American companies for new pending privacy compliance as well as result in both compliance **and** security.

Once Americans better understand the European view of data privacy, we will be better able to address the issue of equilibrium between US-EU privacy and free expression, and debate ethical issues such as who should hold dominion over personal information—you or the free market.

HISTORY OF PRIVACY IN EUROPE SINCE WORLD WAR II

In 1948, the United Nations passed the Universal Declaration of Human Rights, which recognized a need to balance privacy and free expression. Although Americans also enjoy these fundamental rights, Europe experienced a reality during the 20th century when personal privacy was a life-or-death matter. As a result, privacy in Europe was given preference over free expression. Recent European cases such as the Irish Anti-Blasphemy prosecution of Stephen Fry or the possibility of criminal prosecution under the Treason Felony Act 1848 for public calls advocating the abolition of the British Monarchy are unthinkable to most Americans. While these laws surely have detractors in Europe who may categorize them as archaic and outdated, they are still in force and effect today.

Similar to the United States Bill of Rights, the European Convention on Human Rights (ECHR) was passed by the Council of Europe in 1953. It provided a broad scope of fundamental rights similar to those articulated in our own founding principles. These fundamental rights included (in part) a right to life, liberty, and security; respect for private and family life; freedom of thought, conscience, and religion; freedom of expression; freedom of assembly and association; right to marry; right to an effective remedy; and prohibition of discrimination. Additionally, these fundamental human rights were enforceable in the European Court of Human Rights based in Strasbourg.

Based in Luxembourg, the European Court of Justice (ECJ) is another high European court also dealing with privacy cases. Decisions from both the ECJ and the ECHR are binding on the European member states and can lead to legislative changes by national governments similar to the power that the US Supreme Court has over state and local government decisions.

Although Europe now had the equivalent of a “Supreme Court” with the ECJ and ECHR, the next few decades were marked by each European member state passing its own version of privacy rights much the same way the US struggles with data breach notification laws for each state. The rise of the computer in the 1970s along with the need to transact business among disparate European communities brought about OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data released in 1980 and updated in 2013. The ECHR and ECJ both addressed various privacy cases to establish precedent in the European Union and European Economic Community (EEC).

Some of these cases included Google Spain vs. AEPD and Mario Costeja Gonzalez (2014), which ordered Google to remove a link to an article containing personal data in online archives; Halford vs. UK (1997) and Copland vs. UK (2007), which dealt with employee monitoring in the workplace; and Bodil Lindqvist v Åklagarkammaren i Jönköping (2003), which addressed whether information stored in one country but made accessible over the internet should be considered a transfer of data to a third country.

To address the exchange of personal data between the EU and the United States, the European Commission and the US Department of Commerce developed “Safe Harbor” as a self-regulatory framework to ensure adequate privacy protection for transatlantic data transfers. In July 2000, the European Commission determined the Safe Harbor Privacy Principles complied with European Data Privacy laws and allowed EU personal data to be transferred to US-based companies. However, the combination of Safe Harbor’s unreliable self-certification mechanism, lack of compliance enforcement by the FTC, and Edward Snowden’s 2013 disclosure of mass surveillance operations by the NSA led the European Court of Justice to strike down Safe Harbor in its Max Schrems v. Data Protection Commissioner and Digital Rights Ireland 2015 decision. The case was brought by Maximillian Schrems against Facebook Ireland for transferring personal data to the United States without adequate protection.

In 2016, the European Commission and US Department of Commerce released the EU-US Privacy Shield Framework to address some of Safe Harbor’s weaknesses, but the new framework has not yet been deemed adequate through the European Court of Justice and multiple challenges are pending to protect the fundamental privacy rights of Europeans.

HIDDEN PRIVACY DANGERS

Let’s step back for a moment. Why is privacy so important that Europeans consider it a fundamental human right, even in the private sector? After all, there’s no harm done in sending some coupons to a pregnant teenager.

Or is there?

To illustrate the danger, consider the consequences when our ability to make informed decisions is corrupted or when we don’t have the opportunity to correct the record. For example, let’s consider a happily married woman working in a male-dominated field who recently started her own business. Google, Waze, Apple, and all the apps on the family’s phones tracked her location and some purchase activity.

Before we tell the story about our example, remember that those companies share data “to improve customer experience and the relevance of ads” as commonly described in privacy consent notices without much detail. Even when companies ask for consent to access profile information through an app or website, many US-based apps default to liberal data sharing policies. However, a lot of profile information is also obtained without a consumer’s consent. Technology companies such as InfoUSA recognize the value of aggregating and selling or exchanging profile information to improve customer profile data. This data may include information gathered without the customer’s consent such as details about the consumer’s ethnicity, age, gender, spouse, children, and other demographic information.

This enhanced profile information is bought and sold to anyone wishing to gather intelligence such as banks, insurance companies, retailers, individuals, and even other data aggregators. Other companies specializing in data analytics and predictive algorithms with the aim of influencing user behavior churn the data from these intrusively personal profiles into the "enhanced customer experiences" touted by a product or service provider.

Back to our example, one of the data aggregators noted that the woman seemed to meet a lot of men for coffee and lunches. That data aggregator sold access to her profile data to any retailer willing to pay for information about consumers looking for "people traveling within a zip code," "people who drink coffee," or "women over 40." Afterward, the ads for Starbucks and Panera she received were helpful but she also received ads for Match.com and other dating websites—even though each of her meetings was for an entirely legitimate business purpose.

There was no way for the woman to object or gain transparency into who created the profile, how the algorithm works, its accuracy, or to whom it was shared. The woman's husband then received ads on his phone from Ashley Madison and shady divorce attorneys who recognize value in creating conflict to drum up business. These businesses purchased data on "married working people" or "couples married more than 7 years" or "spouse location data and purchase history" and combined the lists. The end result, right or wrong, suggested that his wife had been stepping out on him.

So, no risk?

Suppose the couple now considers a major purchase and needs a loan. The bank determines loan risk and credit worthiness based on a comprehensive profile of the prospective borrower and purchases enhanced profile data—not just from the credit reporting agencies (such as Equifax, TransUnion, and Experian) but also from multiple data aggregators. Based on the purchased enhanced profile data for this couple, the bank determines the financial risk associated with a soon-to-be divorced couple is higher than that of a married one, and so the couple receives less favorable loan terms.

If this example seems far-fetched, you are only beginning to understand why Europe takes privacy so seriously. Although individual data points may be limited in their usefulness, combining profile data from other sources is extremely insightful and largely unregulated—and may have a financial impact on an individual or family. Some aggregators in this example may have figured out the woman was just trying to build her business, as evidenced by a recent filing in the Secretary of State's office earlier that year. However, others found that data point irrelevant and excluded it from their algorithm. After all, the algorithms used to determine loan risk are considered intellectual property by the bank and may not necessarily be accurate or fair. When a group believes illegal discrimination occurred in determining credit risk or other financial

decisions, the dispute is often only remediated through legal action and negative media attention.

Retail and financial institutions are not the only industries to base their decisions on profile data. Online business news publisher Quartz (qz.com) accurately stated in a September 2018 article that "No one wants your data more than your health insurer." To extend our example, the couple's health insurance company uses profile data to determine that the wife must have an unhealthy addiction to caffeine given the number of times she visits Starbucks in a given week. Coupled with the likelihood of stress-related illness from the pending divorce, the health insurance company decides to increase their premiums next year or drop their coverage entirely. Sure, maybe she only ordered herb tea or water for a number of those Starbucks visits, but the insurance company will choose to make conservative decisions and treat each visit as a caffeine ingestion in their algorithm.

This example illustrates that the personal consequences of unregulated data privacy can become arguably much worse than a stolen credit card or bank account. Under US law, banks are required to make consumers "whole" when their identity and financial information has been compromised. Financial institutions usually refund fraudulent charges and issue new credit cards within hours. Actual out-of-pocket loss to a consumer is limited.

However, incorrect profile information that leads to higher loan terms or insurance premiums can go on for years without consumer discovery. From a security perspective, profile information is a goldmine for social engineering and spear phishing campaigns. Most alarming are the safety concerns with the widespread availability of profile information. Today, someone like Rebecca Schaeffer's stalker could have purchased profile information online with very little resistance—and without needing access to DMV records to find her address.

Similarly, health records such as prescription information, medical diagnoses, and test results are considered Protected Health Information records ("PHI"), but health insurance companies can also gather information from your online shopping grocery lists, recreational interests, location information, and other data. This profile information may not be "protected" by your insurer but is definitely useful to them when making decisions. And, it's available on the open market.

DATA EXCHANGE IN A GLOBAL ECONOMY

We all participate in a global economy that provides instant access to information over the internet from anywhere in the world, including access to profile information. Problems surrounding the exchange of data between countries arises when the commoditization of personal information drives the economy in one part of the world but

is respected as a basic human right in others. As we see from our example of the couple, real privacy consequences exist for what most Americans see as non-threatening data collection but that Europeans have understood as a serious threat for decades.

Europe's GDPR and its predecessors sought to protect consumers from many of the privacy risks highlighted in our example. Perhaps the reason the US seemed to miss out on the international debate over privacy rights was because, as a single unified country, we had not struggled with domestic transborder data flow challenges as seen in cases such as Max Schrems v. Data Protection Commissioner (2015). Whatever the reason for the misalignment, everything changed in May 2018 when GDPR compliance enforcement began and many American companies found their business models incompatible with the European mindset surrounding personal data privacy. Understanding the expectations of the European consumer and adopting the OECD principles as design criteria will help companies design solutions with universal appeal that comply with even the most restrictive privacy regulations in the world.

A PRIVACY "BILL OF RIGHTS"

The OECD Privacy Principles read like a "Privacy Bill of Rights" which are quoted in the table below:

THE OECD PRIVACY PRINCIPLES
COLLECTION LIMITATION PRINCIPLE
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
DATA QUALITY PRINCIPLE
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
PURPOSE SPECIFICATION PRINCIPLE
The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

USE LIMITATION PRINCIPLE
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
a) with the consent of the data subject; or
b) by the authority of law.
SECURITY SAFEGUARDS PRINCIPLE
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
OPENNESS PRINCIPLE
There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
INDIVIDUAL PARTICIPATION PRINCIPLE
An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
ACCOUNTABILITY PRINCIPLE
A data controller should be accountable for complying with measures which give effect to the principles stated above.

Once you understand the value of personal information, the necessity of the OECD Privacy Principles is self-evident given the possible consequences to the consumer. Among these principles, the Data Quality and Individual Participation Principles provide rights to delete and/or correct profile information and a right to challenge how data is being used. Collection limitation, purpose specification, use limitation, and openness all provide transparency in the use, collection, and exchange of personal data while security and accountability address the oversight and governance of personal privacy data.

An economy that incorporates the free flow of information across international borders requires a uniform standard for data privacy. When considering a universal standard, it seems that Americans are more likely to accept gaining privacy protection rights than Europeans are to surrendering them. American companies will need to “up their game” on privacy rights to remain competitive, and the required changes are sure to disrupt the status quo because global American companies have built their businesses on the buying and selling of profile data.

Going forward, adopting the OECD Guidelines as design criteria will go a long way toward inoculating business against the impending sea change. January 28 is recognized internationally as “Data Privacy Day,” commemorating the signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. With privacy dominating headlines in 2018, Americans are ready to embrace the change.

In Part II of this whitepaper, we will examine the legal challenges of implementing a universal privacy standard. Let the NTSC know what you think 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 and ITIL certifications and is a graduate of Auburn University with a Bachelor of Science in Electrical Engineering.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION