Understanding the Issues of Personal Data and Privacy in the European Union and the United States

Marc A. Kowtko

Pace University, Seidenberg School of CSIS, Pleasantville, NY

Abstract

In an era where the Internet has globalized our economy and social networking sites have dominated the social atmosphere; there has been an ever increasing influx of personal data being collected from Internet users. Despite this mass aggregation of data, the issue of privacy has been an increasing concern. What rights to United States (US) citizens have that safeguard their privacy, especially in regards to the collection of their personal data? Studies have shown that more than 75% of European Union (EU) nationals are concerned about the collection and misuse of personal data [1]. This directive serves as a guideline for each of the member states when establishing data protection and privacy laws [2]. Recent news from the EU, especially from the European Commission, has reported the Data Protection Directive is set to change [3]. This research will discuss the privacy concerns of Europeans and Americans and privacy laws that affect both regions.

Keywords—European Union Data Protection Directive, 95/46/EC, European Commission, Data Protection, Data Privacy, Privacy

1. PRIVACY CONCERNS IN THE U.S.

A. The start of the Internet and Concerns Over Personal Data

In 1992, Tim Berners-Lee of the European Organization for Nuclear Research (CERN) developed the World Wide Web. For the first time, this technology allowed the information on the Internet to be clearly illustrated onto a computer terminal screen. Since then, there are approximately two billion users online visiting more than 600 million web pages and completing more than 20 online transactions a minute [4]. The Internet has also become the playing field for social media. In 2003, social networking sites, including MySpace, Facebook, and Twitter began to appear. Now sporting more a billion users, these social networking sites have dominated users’ computer screens, mobile phones, and personal interactions. With all of these transactions occurring, it would seem likely that privacy is important concern for Americans. However, according to the Ponemon Institute, only 51% of Americans are concerned about the collection of their personal data by private corporations and institutions. These concerns have been increased especially with the increase in cyber-attacks against public and private websites. [5].

B. The Lack of Transparency in Contract Law

Despite these concerns, many Americans are still sharing personal data for the world to see. From shopping to social networking, many Americans are failing to realize the amount of personal data they share. For instance, grocery stores often offer discount cards to new or returning customers. Their applications often require customers to give their address, phone number, and email. While this collection maybe needed to send coupons and other discounts; this information may be shared to 3rd party distributors. This can also apply to credit card, mortgage, or lottery/jackpot applications. Often, these types of applications will have a privacy policy or statement link directly on the application. These policies are unclear, contain legal definitions and syntax complexity, and are long; thus many Americans become confused and disregard reading the message all together. By signing the application, they have essentially formed a contract. According to US Business Law, applicants, who are adults, are expected to read the full terms and conditions of the agreement. The disregarding of privacy statements often cannot release the consumer from a valid binding contract [6]. In this case companies of the application agree to allow the consumer to use its services; in return, the consumer allows the company to collect their data on the companies term specified in the agreement. This lack of transparency and lack of understanding of American Business Law harms the average American consumer. Despite this, corporations continue to take advantage of consumers and their privacy.

Some corporations even create a false sense of security and privacy. Although legal, depending on its scope and intentions, this further creates confusion amongst consumers. For example, Microsoft recently aired a campaign stating that their products and services offer more privacy than Google [7]. While that may be true to an extent; Microsoft like others does have non-transparent policies. Only recently have more Americans become concerned about these non-transparent through the use of Mobile smartphones and their applications. Many Americans wonder, “What Constitution rights do we have that protect our privacy?”

C. Privacy Laws and its Implementation in U.S. Society

The Constitution was ratified in 1788 to address the legal powers and limitation of federal government. Unfortunately, there is no explicit amendment or section that explicitly states
the boundaries or definition of privacy. Some legal scholars have stated that there is some non-explicit right privacy. For instance, in the 3rd Amendment, scholars note that this protects homeowner’s expectation of privacy. Created in response to the French and Indian War and the American Revolution, no soldier could forcefully lodge into colonial’s home. The 4th Amendment, which protects citizens from unreasonable seizures, also provides some form of security. This amendment protects citizens from governments eavesdropping into the home or personal lives without reasonable ground and a search warrant [8].

Despite, these interpretations, the lack of a specific amendment has resulted in U.S. privacy laws that are specific and do not extend beyond their limitations. Some of these explicit privacy laws include the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Electronic Communications Privacy Act are just a handful of laws implemented on the federal level of the United States government. The Health Insurance Portability and Accountability Act (HIPAA) was created in response to national health reforms and the introduction of the Electronic Medical Record (EMR). This law established the legal standards for the transactions of patient EMR records between health care providers, insurers, and employers. In addition to addressing the prevention of healthcare fraud, this Act established privacy and security rules. These rules required holders of EMR records to require consent for the disclosure of records to healthcare providers and required adequate security measures for the protections of EMR records held by the providers, insurers, and employers. Another notable law is the Gramm-Leach-Bliley Act of 1999. This act which notably adjusted the regulations amongst investments banks also required financial institutions to protect customer’s personal data and privacy from foreseeable security threats (e.g. cyber-attacks, fraud, etc.). The Electronic Communications Privacy Act restricts the federal and private entities on methods of intercepting data. Data collected must also contain reasonable privacy protections [9]. The US PATRIOT Act, enacted in 2001 under then President George W. Bush, largely removed this requirement amongst federal and law enforcement agencies [10].

While these laws address some concerns over the collection and use of personal data, even online; advocates still signaled that a more comprehensive bill was needed. In 2011, the Commercial Privacy Bill of Rights Act was introduced into Congress. Similar to the EU’s Data Protection Directive, this law would afford citizens certain data protection and privacy rights. This bill would also regulate businesses that collect and process personal data. Unfortunately, the bill died; it has yet to be re-introduced [11]. Data collection and privacy continue to be a major concern in the US, especially for consumers and companies alike.

2. ACROSS THE GLOBE: DATA PROTECTION IN THE EU

A. The History of Europe and its Effect on Data Collection

As stated in the Introduction, more than 75% of EU citizens are concerned about the collection and misuse of their personal data. You may ask, “Why are more Europeans concerned about their data?” Many scholars have noted that perhaps the EU’s response is largely to blame on Europe’s history, especially the eras of World War I, World War II, and the Communist era in the Eastern region of Europe. During these turbulent times, both governments, political, and labor unions collected personal data of Europeans and used their information to harm Europeans. During the Nazi Germany era, millions of citizens of Jewish descent had their personal data collected. This information was used to identify, persecute, and even execute millions of European Jews between 1940 and 1945, the Holocaust. After World War II, Europe continued to be separated between the “Capitalist West” and the “Communist East” European regions. It is apparent the history is an important part of European society. For Europeans, this turbulent and sometimes deadly past explains their concern of data collection [12].

B. A brief Understanding of the European Union Data Protection Directive (95/46/EC)

In 1995, the European Commission’s Data Protection Directive was ratified. This directive serves as a guideline for each individual EU member states to impose data protection and privacy laws based on the context of the Data Protection Directive. To summarize the Directive as a whole; privacy is a human right. No citizen can be deprived of privacy [13]. There are seven key principles that are focused in the Directive. The first principle in notice; public and private entities who wish to collect data from EU nationals must be notified before any data is collected. Purpose; entities who wish to collect personal data must state a purpose for collecting the data; Explicit consent is required in order data to be collected. Security; entities, both public and private, must implement security plans and register their activities with the government. Disclosure; should a user’s data be subject to disclosure to a 3rd or outside party, that user should be notified and provide explicit consent. Access, users have the right to access their personal data and correct that data should there be a correction needed. Accountability; entities that collect and retain data are held accountable, both criminally and legally, should personal data be compromised [14]. In addition, unlike US privacy laws, the EU Data Protection Directive is generalized and its terms and jurisdiction is set on a broad basis.

3. TRANSFORMATION – DIRECTIVE TO REGULATION

A. Revising and Updating the Directive to Meet the New Challenges of the 21st Century

Despite this directive and its effects on the collection and sharing of personal data in Europe, the EU Commission is set to revise the Directive and transform it into a regulation. By transforming into a regulation, all EU member states must ratify the new law. Essentially this supersedes all previous data protection laws in the European Union and its individual member states. According to the EU Commission, this regulation is designed to reduce overall business costs by requiring EU businesses to follow one mandate then following multiple individual mandates. EU nationals who live in
another EU country outside their home can afford the same protections. EU nationals will have greater information on the collection of their personal data including the “right to be forgotten”. Should an individual deem that their data is no longer needed for its intended purpose, that individual has the right to have all personal data purged or removed from entities that initially collected their data. Individuals who have their data compromised will be immediately informed and may be entitled to compensation. [15].

Currently, the European Data Protection Regulation is currently being revised and examined by each EU member state. These member states evaluate the proposal a suggest revisions if required. Speculators suspect that EU Data Protection Regulation will be ratified at the earliest in 2015 [16]. It is unclear when the European Parliament ratify and replace the current directive. However, across the globe, other nations are concerned primarily the United States.

B. Effect of the EU Data Protection Regulation and the U.S. Economy

While it is unclear when or exactly how U.S. companies, especially exporters, will be affected by the new regulation, researchers and legal analysts suggest companies will be required to have data controllers and Data Protection Officers. Data controllers monitor the data collection process and Data Protection Officers oversee and enforce regulatory compliance of privacy matters. Companies will be under the jurisdiction of a single data protection authority. This is especially troubling since current EU/US safe harbor policies and programs protect US companies from direct European prosecution. Companies would be required to allow EU national customers to have complete access and the right to modify their data should there be an error. Finally, companies would be required to destroy all data of an individual should they claim, “the right to be forgotten”. Lawmakers in the US are closely monitoring the status in Europe [17].

As the Internet and social media continues to expand, the collection of personal data continues, and the concern of privacy matters increase; it is imperative that global society, their leaders, and their governments work together to ensure that citizens’ rights are respected and the innovations of the Internet are not impeded. When a common goal is achieved and society is harmonized, everyone benefits.

REFERENCES

[9] [2]
[10] [8]
[15] [3]