2015

What is Personally Identifiable Information?

Dana Gieser

Introduction

Retailers from around the world have taken to the internet to reach more of the market and increase their overall revenue and bottom line numbers. The internet has created the world of electronic commerce, or e-commerce, and has served as a conduit for merchants and consumers alike to buy, sell, and trade merchandise online. For the first time, the procuring and selling of products has reached a global level, no longer confined by the brick and mortar mentality that used to accompany business. However, with this new medium for trade comes with a host of legal issues for companies to navigate.[1] Prominently located amongst these issues is that of personally identifiable information. More specifically, the requirements of companies to collect and protect this information from potential computer hackers and fraudsters that could use the information to assume a new identity, or use it in other means to the detriment of another. This requires companies to understand difference key regulatory approaches to implementing and successfully managing privacy information in a global marketplace, reliant upon cross-border information flows.[2] The extent of understanding required for this information flow will be outlined, albeit briefly and limitedly, in this paper.

This paper seeks to reconcile the requirement to collect personally identifiable information in order for American companies to partake in the world of international e-commerce, while complying with international laws regarding its safeguard and

---

1 David Baumer et al.; *Internet Privacy Law: A Comparison Between the United States and The European Union,* 23 COMPUTER & SECURITY, July 2004, at 400, 404.

2 Id at 400.

protection. First, it is important to look at what personally identifiable information is and how it is defined differently by different jurisdictions. In most cases, the definition is coarse and every changing.[3] However, there are several key threads that run throughout most statutory law regardless of jurisdiction. Next, it is necessary to understand how different jurisdictions require that companies collect, store, and maintain this information. After the statutory requirements are established, it begs the question of how American companies ensure they are complying with the law when different jurisdictions have different requirements. Finally, this paper seeks to understand what happens when companies fail to comply with these laws. The law is incredibly unclear in regards to what country claims jurisdiction and which, if any, penalties are actually enforceable to a country not domiciled in that jurisdiction.

It is also important to note that while there is a good deal if intersection between different American and foreign laws, there is also a great gap that can make it difficult for some companies to navigate the ever-changing legal and social landscape of privacy protection. In many cases, social and cultural norms play a factor in the creation and verbiage behind privacy laws.[4] It would be "impossible to understand the privacy concerns in the EU without understanding how history has influenced European values, for example, how Nazis used centralized collections of PII to round up and dispose of 'undesirables.'"[5] While the United States is just coming around to the idea of privacy

---

3 Id.

4 Id.

5

and privacy protection, the EU Information Directive of 1995 and the 2002 EU Directive "repeatedly, and emphatically, state that EU residents are entitled to a right of privacy."[6] While this paper is topical and does not linger on the social and political forces that may drive legislation, it would be remiss not to mention it.

This paper does not seek to explain or provide a solution for every country and every circumstance. With the varying laws and interpretations, the scope and magnitude would become too great, and the connections and understanding would become too attenuated. This paper is a survey and cross-section of the personally identifiable information laws of the major trading partners of the United States. This analysis uses Canada, Australia, the United Kingdom, and the European Union countries of Germany, Belgium, and France, to explore the varying world of personally identifiable information in the global context. These countries were chosen due to their large e-commerce relationships they have with United States retailers and merchants. According to Borderfree, Inc., a leading e-commerce company connecting American merchants such as Macy's and Saks Fifth Avenue to international consumer ranks the Canada, Australia and the United Kingdom as their top three market places for global e-commerce.[7] American law is only used to give a guiding perspective on how unregulated the world of

---

[6] Tracie B. Loring, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, TEX. INT'L L.J., 421, 423, (2002).

[6] David Baumer at 402.

[7] INTERNATIONAL ECOMMERCE FASHION: WHAT'S TREDNDING ONLINE?, http://www.borderfree.com/global-insights/international-ecommerce-fashion-whats-trending-online, (last visisted Mar. 8, 2015).

personally identifiable information is compared to the rest of the world. Additionally, the general and non-binding guidance from various politico-economic groups, such as the European Union and the Organization for Economic Co-operation and Development, to under different terminology for the purposes of this paper. Using these countries, this analysis seeks to make sense of the laws of these countries to the world of personal identifiable information.

What is personally identifiable information?

This question, on its surface, may appear to be the easiest questions this paper seeks to answer, but, in fact, is the most difficult of all. Before a company can create internal controls and processes to ensure that personally identifiable information is being protected, it needs to understand what personally identifiable information is. When dealing in the world of international e-commerce, a company needs to understand the definition of many different countries and jurisdictions. For example, an American company doing business on a global level needs to understand the American definition of personally identifiable information, as well as the global definition of it. Unfortunately, for American companies, this definition, both internationally and domestically, is very unclear.

Governments from around the world have varied definitions on what international electronic commerce really means. There is no "widely accepted, specific definition for international electronic commerce."[8] For example, the United States Government

---

8 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-02-404, INTERNATIONAL ELECTRONIC COMMERCE: DEFFINITIONS AND POLICY IMPLICATIONS (2002).

Accountability Office has laid out several examples of what international e-commerce could mean. Amongst these examples are: "(1) the purchase of a book ordered over the Internet from Amazon.com by a French customer, for delivery in Paris" or "(4) the purchase of office supplies from a U.S. company, using an on-line auction service, for delivery to a business in Canada." [9] Generally speaking, international e-commerce constitutes any "on-line orders generate the cross-border movement of goods or services."[10] Whenever an American company sells goods or services to anyone outside of the United States, it has engaged in the practice of international e-commerce, and therefore, must abide by specific rules to safeguard the information collected to complete said transaction.[11] This information is more commonly known as personally identifiable information.

There is no American federal law that defines what personally identifiable information is specifically within the e-commerce world. In other words, there are no statutes, written and passed by Congress and signed by the President of the United States, which outlines any or every piece of information that is, or could be considered personally identifiable information. The only statutory law that even applies specifically to the Internet is the Children's On-line Privacy Protection Act of 1998 (COPPA), which is less about international e-commerce, and more about prohibiting "unfair and deceptive

---

9 Id.

10 Id.

11 Id.

practices in connection with the collection and use of personal information from and about children on the Internet."[12] In 2003, Senator Frelinghuysen from New Jersey introduced the Online Privacy Protection Act, which would have "require[d] the Federal Trade Commission to proscribe regulations to protect the privacy of personal information collected from and about individuals not covered by COPPA."[13] Within in this legislation, Congress, in Section 8(8), had defined personal information as "first and last name; home and other physical address; e-mail address; social security number; telephone number; and any other identifier that the Commission [FTC] determines identifies an individual; or information that is maintained with, or can be searched or retrieved by means of, data described immediately above."[14] Additionally, he proposed the Social Security On-line Privacy Protection Act in 2003, which would have made the "disclosure of social security account number or related personal identifiable information without consent prohibited" by an interactive computer service.[15] Both of these pieces of legislation died in committee, and therefore, left no tangible trace of a true legislative definition of personal identifiable information.

Where federal legislation is lacking, however, different administrative agencies created by the federal government have begun to pick up the slack. According to the

---

12 16 C.F.R §312.1

13 MARCIA S. SMITH, CONG. RESEARCH SEV., RL31408, INTERNET PRIVACY: OVERVIEW AND PENDING LEGISLATION 4 (2003).

14 Online Privacy Protection Act of 2003, H.R. 69, 108th Cong. §8(8) (2003).

15 Social Security On-line Privacy Protection Act, H.R. 70, 108th Cong. §2 (2003).

Office of Management and Budget, personally identifiable information is defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[16] However, this definition was laid out in a footnote, a sidebar to explaining the need for government agencies to do their due diligence in safeguarding the information of American citizens, to prevent breaches from outside forces.[17] It was never intended for the use and collection of information within the world of e-commerce. On the other hand, since is the closest "official" definition, on record, it will be used as the baseline for how American e-commerce companies should understand personally identifiable information. Additionally, since it seems to mirror quite closely the definition laid out by Senator Frelinghuysen, it is the definition that is accepted as the "American" definition for the purpose of this paper.

On a state level, several states have begun to propagate statutory laws that outline and define what personally identifiable information is. For example, California created an Online Privacy Protection Act (COPPA) of 2003, which provides exact examples of what defines personally identifiable information and the different protection enforcement considerations that they require for companies operating in California to be compliant.

---

16 OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, SAFEGUARIDNG AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION, M-07-16 (2007).

17 Id.

The California law essentially uses the same parameters that the unsuccessful federal OPPA used, almost verbatim. Specific examples California has chosen to outline are:

> (1) a first and last name; (2) a home or other physical address, including street name and name of city or town; (3) an e-mail address; (4) a telephone number; (5) a social security number; (6) Any other identifier that permits the physical or online contacting of a specific individual; and (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.[18]

California has some of the strictest definitions in terms of what constitutes personally identifiable information. Unfortunately, these rules only apply to "a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service…"[19] They do not apply to any other situation in which the person resides outside of California. Additionally, since this is state law, it does not bind companies

Unfortunately for most companies, what constitutes personally identifiable information on an international level is even murkier and less explicit. A guiding principle for most countries begins with a branch of the United Nations known as the Organization for Economic Co-operation and Development (OECD). With thirty-four nation states, including all that will be explicitly analyzed and discussed in this paper, the

---

18 2004 Cal. Stat. 22575-22579.

19 Id.

OECD created their own guidelines for what personal identifiable information is.[20] In the annex to the Recommendation of the Council of 23rd September 1980, "'personal data' means any information relating to the identified or the identifiable individual (data subject)."[21] The vague nature of this definition is reminiscent of the United States and their vague definition. Following the OECD definition, any information at all collected would be considered personal identifiable information and has to be collected and stored. This is the only definition ever promulgated by the OECD, and one that has been most accepted by its member countries, even 30 years later.

Australian law is a direct offspring of this OECD recommendation. Under the Privacy Act of 1988, Australia attempts to outline what can be considered personal information.[22] The law states that personal information "means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."[23] Australia's definition lays out that it does not matter if the personal identifiable is true or not, any information that could identify an individual should be treated as protectable personally identifiable information.

---

20 ABOUT THE OECD, http://www.oecd.org/about/ (last visited Feb. 8, 2015).

21 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sep. 23, 1980), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

22 *Privacy Act 1988* (Cth) S 1.

23 Id at div 1, s 6, ss 1.

For the American company, this also means that even if the consumer provides information that is incorrect, it is still the job of the merchant to treat it as personally identifiable information and treat it as such.

Europe has also taken the guidelines of the OECD and by go a step further, creating their own definition of what constitutes personal data. Under Article 2 of the EU Data Directive (95/46/EC), personal data is defined as "any information relating to an identified or identifiable natural person ('data subject')."[24] The directive, in the same article, continues on to define what is an identifiable person as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[25] Under this definition, companies could be required to consider any and all information provided by the customer to the merchant for transactional purposes. Under this extreme version, a merchant inherently becomes responsible for any piece of information reported by the customer to the merchant, creating a potential web of issues for compliance purposes.

Additionally, within the European Union, each country has their own legislation based on the adoption of the EU data protection policy which has its own definitions of personally identifiable information. In some cases, the data privacy laws of the country predate the EU Directive. In these cases, countries like France and Germany, discussed

---

24 Council Directive 95/46/EC, 1995 (L 281) 0031-0050.

25 Id.

below, maintained their privacy laws as they fell into accordance with the Directive. Interestingly enough, the EU directive seems to have derived from these pieces of legislation as the language is similar in nature. Other countries, such as the United Kingdom and Belgium, also discussed below, wrote their legislation to be in accordance with the EU Directive. The language of these adoptions is actually much more varied from the original language of the Directive. The thing that all of these documents have in common in the room for interpretation by a company trying to determine what the personal identifiable information is.

Some countries continue to rely on their privacy laws that predate the EU Directive of 1995, as the language in their privacy laws already encompassed the language of the Directive. For example, The Commission Nationale de l'Informatique et des Libertés (CNIL) is administrative branch of the French Government which monitors and enforces the data protection laws within the French Republic.[26] Relying on Act N°78-17 of 6 January 1978, through subsequent amended documents the agency carries through the definition of personal data as "any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him."[27] Similarly, the Bundesdatenschutzgesetz, BDSG, also known as the Federal Data Privacy Act, defines personal data as "any

---

26 Role and Responsabilities, http://www.cnil.fr/english/the-cnil/role-and-responsabilities/ (last visited Feb. 15, 2015).

27 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 2008 on Information Technology, Data Files and Civil Liberties] JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O], Jan. 6, 1978, p. 7.

information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).”[28] This Act, passed originally in 1980, and has since been amended, continues to use the same personal data language from the original document.[29] In both cases, the terms identifiable and identified are used in the same vein as the EU Directive and therefore, allows the definition to be maintained after the Directive is issued.

In other cases, however, countries created legislation following the Directive. These countries adopted the language in some form or another, but unlike the countries with privacy laws prior to the Directive, chose different terms and definitions to define what personal data is. In 1998, the United Kingdom passed the Data Protection Act of 1998 to adopt the verbiage and premises of the EU Directive.[30] Under Part I of the Data Protection Act, personal data is “data which relate to a living individual who can be identified – (a) from those data…”[31] However, Belgium, when adopting the EU directive, created a more in depth and complicated version of what constitutes personal data, which is just as ambiguous as the EU Directive in a very different way. In the Belgian Royal Decree of 2001 regarding privacy protection divides personally

---

28 Gesetz zum Schutz vor Mißrauch personenbezogener Daten bei der Datenverarbeitung [Law on Protection against misuse of personal data in data processing], December 20, 1990, BGBl. I 1990 S.2954.

29 Id.

30 Data Protection Act, 1998, c29 (U.K).

31 Data Protection Act, 1998, c29, §1 (U.K).

identifiable information into two categories: "encoded personal data" and "non-encoded personal data."[32] Encoded personal data is "personal data that can only be related to an identified or identifiable person by means of a code."[33] Non-encoded personal data refers to "data other than encoded personal data."[34] In this case, the term "identifiable" relays directly for someone to ascertain the identity of an individual by means of using the information to avail the identity of a person or individual. Both of these countries vary in some way form the EU Directive, but maintains compliance with the overall understanding of it.

Generally any information provided by the customer to the company could be considered identifiable information, and therefore, would fall within the overhead of personal data. Under the EU Directive and all the countries with variations of it, there are no specific examples or guidelines that outline what is personally identifiable information is in those countries. In 2002, the European Union promulgated the "Directive on privacy and electronic communications, which seeks to "harmonise[s] te provisions of the Member States required to ensure… the right to privacy, with respect to the processing of

---

32 Voorontwerp van koninklijk besluit houdende uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens zoals gewijzigd bij wet van 11 december 1998 [Draft Royal Decree implementing the Law of 8 December 1992 on the protection of privacy in relation to the processingof personal data as amended by Law of December 11, 1998] MONITEUR BELGE [M.B], Mar. 8, 1999, 1.

33 Id.

34 Id.

personal data in the electronic communication sector."[35] While the EU directive is well intentioned to attempt to provide clarity for enforcement in the changing electronic world, it fails to provide an updated definition of personal data, instead providing continuous reference to the 95/46/EC definition.[36] Unfortunately for the company selling the product, there is no specific definition, and they are left open to potential misinterpretation or judgment calls. Regardless if a company looks to individual country law, or seeks to find protection under the overarching EU Directives, they would be subject to use their best judgment to interpret what information would be considered personally identifiable information.

Canadian law is similarly unclear. There are two main laws that guide privacy, the Privacy Act and the Personal Information Protection and Electronic Documents Act. The Personal Information Protection and Electronic Documents Act was passed in 2000 was created to "govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[37] This document, which was created to help the e-commerce community, is particular vague in its definition of personally identifiable information, simply defining it as

---

35 Council Directive 2002/58/EC, 1995 (L 201) 0037-0047.

36 Baumer at 404.

37 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).

"information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[38] However, Canada does provide another option for merchants to seek clarity on the definition through the predecessor of the Personal Information Protection and Electronic Documents Act, the Privacy Act.[39] The definition under the Privacy Act, with examples relating specifically to e-commerce states personal information as

> "information about an identifiable individual that is recorded in any form including,… (c) any identifying number, symbol or other particular assigned to the individual,… (d) the address, fingerprints or blood type of the individual,… (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual…"[40]

Companies can use this information to begin to understand what personal identifiable information is under Canadian law. However, similar to their European counterparts, these guidelines are not dispositive, and some types of information not enumerated in the laws may be considered personally identifiable information.

In sum, there is no clear definition to what personally identifiable information is. There are clearly some things that merchants should treat as such. Information such as first and last name, national identification number, address, e-mail address and credit card information are highly likely to be considered PII. However, under the laws of all the organizations and countries above, date of birth, age, and generic country or state of

---

38 Id.

39 Id.

40 Id.

residence can also be considered personally identifiable information. The underlying principle here is that there is no standardized and explicit definition to personal identifiable information. There are a lot of questions and potential possibilities for what would qualify. American merchant should do their due diligence in treating that any information that may identify an individual be close secured and safeguarded against potential security breaches to stay in compliance with all governments internationally.

How does the law protect PII?

Understanding what personal identifiable information is the hardest part. Most countries have left open for interpretation what can and should be considered as PII. However, what countries have not left open for interpretation is how they should protect it. All countries have very specific guidelines for the collection and processing of this data. There are guidelines on how it should be stored, organized, collected, and how it can be processed for dissemination and uses for all different industries. In the ever evolving technological world, it is necessary for companies to adopt the methods of these different industries for their own personal use, as legislative change has generally been slower than technological ones. More importantly, they need to determine how countries require how personal data or personally identifiable information needs to be protected in each respective country. Understanding the law will help answer the final question of this analysis: how governments protect themselves against PII violations.

American law primarily protects personally identifiable information through the Electronic Communications Privacy Act.[41] This Act, in conjunction with the Stored Wire

---

41

Electronic Communications Act are the two American legislative pieces that address protection of "wires, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers."[42] Additionally, this Act applies to "email, telephone conversations, and data stored electronically."[43] While the Act has seen significant amendments due to subsequent legislation, most notably the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 and the USA PATRIOT reauthorization acts in 2006, the definitions are still useful in understanding the small amount of legislative guidance Congress has provided to companies surrounding personal identifiable information.[44]

This Act defines intercept as "the aural or other acquisition of the contents of wire, electronic, oral communication through the use of any electronic, mechanical, or other device."[45] Additionally, "electronic, mechanical, or other device" is defined as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than… being used by a provider of wire or electronic

---

 18 U.S.C §2510-22 (1986).

42 ELECTRONIC COMMUNCAITONS PRIVACY ACT OF 1986, JUSTICE INFORMATION SHARING https://it.ojp.gov/default.aspx?area=privacy&page=1285 (last visited Feb. 8, 2015).

43 Id.

44 Id.

45 18 U.S.C §2510 (1986).

communication service in the ordinary course of its business…"[46] While there are a multitude of other definitions embodied in this Act, these two are the most relevant regarding the collection and use of personal identifiable information for e-commerce merchants. The Act is structured to protect personally identifiable information from illegal interception, or when interception takes place when "one of the parties to the communication has given prior consent to such an interception."[47] It is this focus on consent that drives further discussion around personally identifiable information in the global marketplace.

However, this Act was passed before the time of commonplace internet usage and e-commerce. The archaic nature of it is particularly cognizable in recent litigation surrounding the collection and use of personally identifiable information by one of the largest internet websites, Google. In 2013, the United States District Court for the North District of California granted a motion to dismiss in favor of Google, in which one of the Plaintiff's claims relied upon the ECPA.[48] *In re Google Privacy Policy Litigation*, the Plaintiff's claim, through a class action lawsuit, that Google's amended privacy policy violated their privacy protection and they had suffered an injury-in-fact.[49] They state that

---

46 Id.

47 18 U.S.C §2511 (1986).

48 In RE Google, Inc. Privacy Policy Litigation, Order Granting Motion to Dismiss, (No. C-12-01382-PSG), *available at* http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1589&context=historical.

49 Id. at 1.

Google's sharing of their personally identifiable information to other Google products, without the Plaintiff's consent and collection of information via the use of "cookies" to track user behavior to improve consumer pinpointed marketing, produced harm to them. They relied upon the ECPA to support their claims, noting that "Google's use of the accused devices

to intercept Gmail communications and co-mingle the contents and distribute those contents without consent was not necessary to the delivery of Gmail…"[50] In other words, the distribution of personally identifiable information to other devices and products with the Google network was not necessary to the "ordinary course of business" requirement outlined by the ECPA, and therefore, violated their privacy rights.

The District Court disagreed with the Plaintiff's assertion of claims in regards to the ECPA. The Court notes that the Plaintiff's "narrow read of the exemption, as being limited to only action taken to deliver the electronic communication, does not square with the plain meaning of the statutory text at issue."[51] Put differently, the agreement the Plaintiff's made with Google cannot be looked at in a vacuum, where their use of personally identifiable information cannot and should not be solely limited to its use during email transmission. The Court notes that use of this information for reasons other than email transmission could be considered within the "ordinary course of business" exemption. Additionally, the Court notes that this exemption could not apply "because of

---

50 Id at 19.

51 Id.

their allegations that Google exceed the scope of the consent secured by their agreements with Plaintiffs."[52] The Court additionally did not agree with the Plaintiff's claim that by changing its privacy policy, Google violated the privacy rights of its users. Most notably, the Court states the "ordinary course of business" exemption of the ECPA applies, as Google did not do "anything in secret, but rather it publicly announced a new practice."[53] The announcement of its privacy policy was not "in conflict with its prior representations," and, therefore, fell under the exemption provided in the ECPA.[54]

Additionally, the Plaintiff's in this case relied upon another piece of Congressional legislation in this case, the Stored Communications Act (the "SCA). The SCA regulates when an electronic communication service provider may use "the contents of or other information about a customer's emails and other electronic information to private parties."[55] The purpose of this Act is to prohibit an electronic service provider "from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient."[56] The Act states "a person or entity providing an electronic communication service to the

---

52 Id at 21.

53 Id.

54 Id.

55 PRIVACY: STORED COMMUNICATIONS ACT https://ilt.eff.org/index.php/Privacy:_Stored_Communications_Act (last visited Mar. 10, 2015).

56 S.Rep. No. 99-541, 97th Cong. 2nd Sess. 37, reprinted in 1986 U.S.C.C.A.N. 3555, 3591.

public shall not divulge to any person or entity the contents of a communication while in electronic storage by that service."[57] However, it provides a very important exemption for the world of e-commerce which states "a provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or a customer of such service… with the lawful consent of the customer or subscriber."[58] The District Court barely even recognizes this claim, only to dismiss it without standing *In re Google Privacy Policy Litigation.* The failure of a federal court to recognize a privacy claim based on this piece of legislation, in conjunction with the failures under the ECPA show the lack of strength in the governing law in today's internet world.

The two pieces of legislation mentioned above are the only two pieces of legislation that address the collection and protection of personal identifiable information. There is a third piece of legislation, the Gramm-Leach-Bliley Act, 15 U.S.C §6801, which requires that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[59] However, the Act generally refers to banks and "financial holding companies" and does not address internet sites that participate in financial transactions directly.[60] As a result, this act leaves open

---

57 18 U.S.C §2702 (2012).

58 Id.

59 15 U.S.C. §6801 (2010).

60 12 U.S.C. §1843 (2010).

to interpretation whether or not e-commerce falls under the disclosure requirements laid out In the Gramm-Leach-Bliley Act.

The guidance provided by the Federal Trade Commission Also frustrates the process of understanding how e-commerce companies should manage personally identifiable information. Under Section 45 of the Federal Trade Commission Act, the FTC is charged with preventing "persons, partnerships, or corporations… from using unfair methods of competition in or affecting commerce and unfair and deceptive practices in or affecting commerce."[61] Additionally, in regards to international ecommerce, the Act notes that "for purposes of Subsection (a), the term "unfair or deceptive acts or practices" includes such acts or practices involving foreign commerce that… involve material conduct occurring within the United States."[62] Under this provision, all international e-commerce where the company is based on American soil would be required to be compliant with these regulations. However, while the FTC has the power to enforce and protect individuals and, by extension, their personally identifiable information, they have often relied upon the theory of "self-regulation" in which companies themselves are held accountable for regulating their own privacy policies.

In their 2000 report to Congress entitled "Privacy Online: Fair Information Practices in the Electronic Marketplace," the FTC outlines four general principles for

---

61 15 U.S.C §45 (2012).

62 Id.

consumer-oriented commercial Web sites: Notice, Choice, Access, and Security.[63] These websites that collect personally identifiable information would be required to comply with these fair information practices.[64] Notice denotes that "web sites would be required to provide customers clear and conspicuous notice of their information practices."[65] This would include "what information they collect, how they collect it…, how they use it,… whether they disclose the information collected to other entities, and whether other entities are collecting information through the site."[66] Under choice, "web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use of which the information was provided."[67] Access would require web sites "to offer consumers reasonable access to the information a Web site has collected about them, including reasonable opportunity to review information and to correct inaccuracies or delete information."[68] Finally, security would require web sites to "take reasonable steps to protect the security of the information collected from

---

63 FEDERAL TRADE COMMISION, A REPORT TO CONGRESS, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000).

64 Id.

65 Id at 14.

66 Id at 36.

67 Id at 37.

68 Id.

consumers."[69] These are the four guidelines that the Commission would recommend be made into legislation regarding the practice of collection of personally identifiable information online.

However, at the end of the report, the Commission notes that the "implementation of these practices may vary with the nature and the information collected and the uses to which it is put" and therefore recommends "that any legislation be phrased in general terms and be technologically neutral."[70] Additionally, the Commission "notes that industry self-regulation programs would continue to play an essential role under such a statutory nature."[71] Congress appears to have taken these final recommendations into consideration, as it has not produced comprehensive legislation writing these four guiding principles into law. As a result, these recommendations remain as guidelines under which the FTC operates under Section 5 of the Federal Trade Commission Act.

In 1980, the Organization of Economic Cooperation and Development (OECD) issued the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," which outlines guidelines and principles regarding the safeguarding and sharing of personally identifiable information.[72] Among these guidelines are eight basic principles the OECD recommends all member nations put into national law that balance the flow of

---

69 Id at 9.

70 Id at 37.

71 Id.

72 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

information as well as the privacy rights of individuals. These eight principles outlined include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[73] Additionally, the OECD outlined guiding principles on how member nations should apply these principles to national law. Within their recommendation is that member states. Per the regulations, member states should:

> "adopt appropriate domestic legislation; encourage and support self-regulation, whether in the form of codes of conduct or otherwise; provide for reasonable means for individuals to exercise their rights; provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and ensure that there is no unfair discrimination against data subjects."[74]

In the United States, the 2000 FTC Commission report seeks to begin the implementation of these by suggesting appropriate domestic regulation and encouraging self-regulation. Additionally, their four fair information practices encompass the ability for consumers to exercise their rights. However, this is where American compliance seems to end. Fortunately, the European Union guidelines as well as Canadian and Australian Law provide greater direction and guidance.

The European Union adopted Directive 2002/58/EC on July 12, 2002 concerning the processing of personal data and the protection of privacy in electronic communications sector, also known as the Directive on privacy and electronic

---

73 Id.

74 Id.

communications.[75] This directive seeks to expand upon Directive 95/46/EC which addresses the "protection of individuals with regard to the processing of personal data and on free movement of such data."[76] In many respects, the 2002 Directive only seeks to strengthen the 1995 Directive and apply the concepts provide in the 1995 Directive directly to the internet. Unlike the United States, the European Union requires its member states to create specified legislation that would ensure that certain guidelines and requirements are being met to "ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular to the right of privacy, in order to ensure the free flow of personal data in the Community."[77] These guidelines encompass many of the principles spelled out by the OECD. Additionally, made of the requirements apply directly to companies engaging in ecommerce, and how they must safeguard their consumers.

Unlike the United States, the European Union Directive propagates a length of time and means of storage for all personally identifiable information collected by ecommerce companies. For instance, Directive 2002/58/EC provides that any personal data collected should "not be stored for any period longer than is necessary for the transmission…and that during the period of storage the confidentiality remains

---

75 Council Directive 2002/58/EC at 37.

76 Council Directive 95/46/EC at 31.

77 Council Directive 2002/58/EC at 37.

guaranteed."[78] For ecommerce companies, this information could be confusing, as it is a bit unknown when the transmission begins and ends. However, the Directive goes a step further to alleviate this issue, adding the "exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided."[79] This provides clarity for ecommerce merchants, who could be confused as to when they were required to delete information under the Directive. As long as the information is necessary for billing purposes, they can store and maintain the data securely in their system.

Additionally, the 2002 EU Directive lets stand the "principles for data quality" that the 1995 Directive lays out.[80] The 1995 Directive identifies five criteria that European Union member nations must ensure are in their national legislation in regards to data protection. The first requires member nations to provide that "personal data be processed fairly and lawfully."[81] Second, member states much ensure data is collected for "specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[82] Third, member states must ensure data collected is

---

78 Id at 39.

79 Id at 40.

80 Id at 37.

81 Council Directive 95/46/EC at 40.

82 Id.

"adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed."[83] This provision is a key component for all ecommerce retailers to highlight in their policies, as it regulates *how much* data can be collected, leaving a "less is more" mentality in terms of the data that is collected by companies. Fourth, member states must ensure that data is "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."[84] This regulation guides governmental agencies more than companies. Finally, the fifth requirement is an echo of what the 2002 Directive states in other sections, which requires that data be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[85] This requirement, in conjunction with the third regulation, embody an important principle to the requirements to protect data by member states.

Finally, the 2002 EU Directive imports the 1995 EU Directive in regards to the concept of consent. The 1995 Directive defines "data subjects," or in the ecommerce world, "consumer's," consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him

---

83 Id.

84 Id.

85 Id.

being processed."[86] Additionally, the 2002 Directive leaves intact the requirement that data can only be processed when the "data subject has unambiguously given his consent."[87] This Directive, an all subsequent directives, lay out the premise that a consumer must give a retailer explicit consent to process and store their personally identifiable information for the sake of doing business. This idea of explicit consent will be examined further in Section Three. However, companies should take heed to ensure that their disclaimers regarding consent are clear and understandable, and that the acknowledgement is done by explicit action. For instance, the 2002 Directive notes that "ticking a box when visiting an Internet website" would suffice for providing explicit consent.[88]

The combination of these two Directives gives clarity into three fundamental requirements of European law surrounding the security of personally identifiable information. The first two requirements maintain that ecommerce retailers to only keep personally identifiable information within their systems for as long as the transmission requires. While this is relatively ambiguous, it does give an outline, and more importantly, a best judgment mentality for how long the data storage is required. Additionally, it requires companies to obtain the explicit consent of the consumer before collecting their information. This may be the more important of the two protection

---

86 Council Directive 2002/58/EC at 39.

87 Council Directive 95/46/EC at 40.

88 Council Directive 2002/58/EC at 38.

requirements outlined by the European Union, as this is one leaves no room for violation. Consent must be given through an explicit action, and put in a way that is not confusing to consumers. Finally, ecommerce companies should only collect enough information as required to complete the transaction, and not collect additional or extraneous information, as this may be found in violation of both EU Directives.

Since these guidelines are directives for member states to follow, and not actual legislation, all member states were required to adopt these laws in some fashion, but in their entirety, to be compliant with their membership in the European Union. For instance, Belgium, in full, adopted the provisions of the 1995 Directive in their 2001 Data Protection Act. For instance, Article 19 requires that "prior to the processing operation the data subject must give his explicit consent to the processing of non-encoded personal data relating to him…"[89] This requirement is almost verbatim to the European Union Directive. In addition, Article 57 requires that retailers ensure "that the data is not disclosed to third parties and that it is not kept any longer than necessary for the purpose of the processing."[90] Once again, Belgium imported language directly from the EU. Companies can either reference the European Union Directive or reference the Belgian Data Protection Act when doing business in Belgium for the sake of security purposes.

---

89 Voorontwerp van koninklijk besluit houdende uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens zoals gewijzigd bij wet van 11 december 1998 [Draft Royal Decree implementing the Law of 8 December 1992 on the protection of privacy in relation to the processingof personal data as amended by Law of December 11, 1998] MONITEUR BELGE [M.B], Mar. 8, 1999, 6.

90 Id at 14.

Similarly, the German Bundesdatenschutzgesetz (BDSG) follows the European Union Directive in scope, but unlike Belgium, does not use the same transposed language of the Directive. Germany requires that all companies that "consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, the declaration of consent shall be made distinguishable in appearance."[91] This would appear to allow companies to "click a box," similar to the ideas of consent provided for by the European Union Directive. Additionally, the Germany law states in multiple places, most notably Sections 3, 20 and, 59, that companies can only keep personal data until the data "is no longer required."[92] Section 20 specifically requires that "personal data in data files shall be erased if… knowledge of them is no longer required by the controller [company] of the data file for the performance of his duties."[93] This wording is similar to the European Union Directive as well as the Belgian requires that data is "not kept any longer than necessary for the purpose of the processing."[94] When doing business in Germany, similar to

---

91 Gesetz zum Schutz vor Mißrauch personenbezogener Daten bei der Datenverarbeitung [Law on Protection against misuse of personal data in data processing], December 20, 1990, BGBl. I 1990 S.2954 at §4.

92 Id at §20.

93 Id.

94 Voorontwerp van koninklijk besluit houdende uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens zoals gewijzigd bij wet van 11 december 1998 [Draft Royal Decree implementing the Law of 8 December 1992 on the protection of privacy in relation to the processingof personal data as amended by Law of December 11, 1998] MONITEUR BELGE [M.B], Mar. 8, 1999, 12.

Belgium, a company can look to either the European Union Directive or German law to understand how personal data is protected.

The United Kingdom created their Data Protection legislation mirrored after the 1995 EU Directive, however, they take many of the items and terms and make enforcement them stronger. Similar to Belgium and Germany, the United Kingdom is much more explicit than the European Union Directive in regards to what constitutes consent in regards to processing and use of personally identifiable information. In the United Kingdom Data Protection Act of 1998, a direct result of the 1995 Directive, the First Data Protection Principle requires that "personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless… (a) at least one of the conditions in Schedule 2 has been met…"[95] Additionally, Schedule 2 lists out the only "conditions relevant for purposes of the first principle: processing of personal data."[96] Specifically, the first condition in which the processing of data is acceptable is when the "subject has given his consent to the processing."[97] The United Kingdom, similar to its European counterparts, lists consent as the most important condition for processing to be done properly and fairly. Interestingly, though, the United Kingdom also allows a company to process data if it is necessary "for the performance of a contract to which the data subject is a party, or… for the taking of steps at the request of the data subject with a

---

95 Data Protection Act, 1998, c29 (U.K).

96 Id at §4(3), sch. 2 (U.K).

97 Id.

view to entering into a contract."[98] A company could also argue that, in the event they did not promote a way to receive consent that the consumer and retailer entered into a contract at the purchase of the products and, therefore, processing of data is legal. While consent is not defined by the United Kingdom, the Information Commissioner's Office, a branch of the Ministry of Justice[99] notes that it accepts the 1995 European Union Directive definition, which states "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.[100] Once again, for most companies it appears that when they are in doubt of how to manage consent in the United Kingdom, they can find the correct information by going back to the 1995 EU Directive.

Similar to Germany and Belgium, the United Kingdom essentially adopted the European Union's guidance on the retention of personal data. The Fifth Principle of the Data Protection Act of 1998 states that "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."[101] The vague language of the principle is reminiscent of those from Belgium and Germany. Additionally, the Information Commissioner's Office notes that the "Act

---

98 Id.

99 RELATIONSHIP WITH THE MINISTRY OF JUSTICE, ABOUT THE OCO, https://ico.org.uk/about-the-ico/who-we-are/relationship-with-the-moj/, (last visited Apr. 10, 2015).

100 THE CONDITIONS FOR PROCESSING, https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/, (last visited Apr. 10, 2015).

101 Data Protection Act, 1998, c29, §4(1) and (2), sch. 1 (U.K).

does not set out any specific minimum or maximum periods for retaining personal data."[102] In general, the Office encourages companies to make a judgment on the retention of data based around three general principles: what the "current and future value of the information" is to the company, what the "costs, risks and liabilities associated with retaining the information" are, and what the "ease or difficulty of making sure it remains accurate and up to date."[103] Retailers and ecommerce companies need to look at the totality of the circumstances regarding the value and ability to secure and retain the data in order to determine whether or not it is necessary to retain the data.

The Commission Nationale de l'Informatique et des libertés (CNIL) of France passed their Data Protection Act in January 1978, seventeen years prior to the 1995 EU Directive regarding the collection and use of personal data. However, this does not mean the French requirements surrounding the collection and retention of personal data differs drastically from their French counterparts. In fact, most of the rules surrounding what can be collected, retained, and processed is markedly similar to their European counterparts. Article 6 of Act Number 78-17 ("The Act") requires that very specific provisions be followed in order to process personal data. First, the Article requires that personal data may only be processed if the data is "obtained and processed fairly and lawfully."[104] This provision is simple: only lawfully obtained data may be processed,

---

102 RETAINING PERSONAL DATA, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/, (last viewed Apr. 10, 2015).

103 Id.

104

which should not be a concern for any retailer or e-commerce provider. Secondly, the data must be "obtained for specified, explicit, and legitimate purposes, and shall not be subsequently processed in a manner that is incompatible with those purposes."[105] This provision can be as straightforward as it is confusing for some companies. While the processing of data for a legal transaction and shipment of goods is clearly a "specified, explicit, and legitimate" purpose, this provision is less clear on whether the collected data can be used for marketing and emailing purposes. The provision does allow for data to be retrained for "statistical" purposes provided that the reasoning is "compatible with the initial purposes of data collection."[106] Insofar as use after collection, companies can at least continue to retain the information for understanding their marketing and target populations. The third provision of the Article requires that the data collected be "adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing."[107] Additionally, the fourth provision requires that the data be "accurate, complete and, where necessary, kept up-to-date."[108] Therefore, companies collecting data from French customers should ensure that they are only

---

 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 2008 on Information Technology, Data Files and Civil Liberties] JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O], Jan. 6, 1978, p. 9.

105 Id.

106 Id.

107 Id.

108 Id.

collecting the data required to process a transaction, and that they keep all records up to date, when applicable.

The last provision is the data retention provision, which echoes the provisions of neighboring countries. France, having written their data processing regulations seventeen years prior to the passing of the 1995 EU Directive appears to have set the tone and language for retention that most countries follow. The fifth and final provision of the Article requires that data be "retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed."[109] While this is positive for the sake of uniformity in regards to creating company guidelines regarding data retention, it is the same ambiguity that companies face in other countries in setting a timeline for retention. This open nature can be rectified by understanding the use of the data, and setting the shortest and most definitive timelines possible for retention.

Finally, this analysis would be remiss if it did not acknowledge future legislation being produced by the European Union to standardize the use and processing of personally identifiable information in the increasingly interconnected world. The European Union proposed legislation that would create a unifying legislation that would dictate the nature and protection of personally identifiable information throughout the twenty-eight member states of the European Union. While it imports much of the language from the 1995 and 2002 Directives, such as the guidelines for lawfully processing information, there are also some differences. For instance, Article 6 requires

---

109 Id.

that data is lawfully processed only where "the data subject [consumer in the case of retail merchants] has given consent to the processing of their personal data."[110] Additionally, Article 6 notes that it is also processing is also lawful where "processing is necessary for the performance of a contract to which the data subject is party."[111] These provisions enshrine the notion that in order to do business in the European Union, the controller, in this case a retailer or e-commerce merchant, must have consent in absence of binding contract to retain and process data. Previously, it was suggested by a number of countries that consent *should* be obtained. The new European Union legislation would require it. The law also provides conditions for consent, which will be discussed later in Section 3 of this analysis.

The new legislation requires that "the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of data."[112] Companies will be required to advise customers at the time of entering personal data why they are entering their data, and what will be done with the data upon its collection and processing. In addition, under the new law, in order to "ensure that data are not kept longer than necessary" companies should establish "time limits… for erasure

---

110 Regulation on the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), PARL. EUR. DOC. (SEC 73) 11 (2012).

111 Id at 44.

112 Id at 22.

or for periodic review."[113] This should be provided during the initial notification when obtaining and processing data. More importantly, the legislation provides a "self-check" by companies to ensure they are continuously monitoring, updating, or erasing personally identifiable information from their systems. This clause would inherently take away the ambiguity of previous provisions regarding retention. Finally, this new law would enshrine a brand new concept, which is the "right to be forgotten," which never existed in prior legislation.[114] Essentially, the "right to be forgotten" allows consumers providing personally identifiable information to "have their personal data erased and no longer processed…where data subjects have withdrawn their consent for processing or where they object to the processing of personal data."[115] The new European law strengthens the rights of the consumer, and puts tighter constraints on companies to manage and secure personally identifiable information that are contained in their systems.

The European Union will not be the first to pass such restrictive requirements in regards to the types of data that can be collected, what constitutes lawful processing and retention, and the requirements of consent. In regards to passing legislation specifically surrounding personally identifiable information in the electronic world, Canada is a front runner in keeping up with the times. Schedule 1, "Principles Set Out in the National Standard of Canada Entitled *Model Code For Protection of Personal Information*" of the

---

113 Id.

114 Id at 9.

115 Id at 25.

Personal Information Protection and Electronic Documents Act outlines all the requirements for collection and retention of personal information for Canadian customers. This section requires that companies "shall document the purposes for which personal information is collected in order to comply with the Openness Principle (Clause 4.8) and the Individual Access Principle (Clause 4.9)."[116] The Openness principle require that companies "make readily available to individuals specific information about its policies and practices relating to the management of personal information."[117] The Individual Access Principle requires companies to "upon request" inform the individual "of the existence, use, and disclosure of his or her personal information and shall be given access to that information."[118] Moreover, the individual has the right to "challenge the accuracy and completeness of the information and have it amended as appropriate."[119] Canadian citizens have greater leverage in obtaining and understanding the collection, use, and the retention of their personally identifiable information that other countries have yet to require.

In regards to what information can be collected, Canada is generally on par with its European counterparts. Clause 4.4, titled Limiting Collection, requires the "collection of personal information shall be limited to that which is necessary for the purposes

---

116 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).

117 Id at 43.

118 Id at 44.

119 Id at 44.

identified by the organization."[120] Furthermore, the Clause requires that information "shall be collected by fair and lawful means."[121] Subclause 4.4.1 requires that "organizations now collect information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified."[122] For retailers working with customers in Canada and the European Union, this should sound familiar from what the various European laws state.

Finally, Canada provides a full section regarding consent, including how it must be obtained and when, and the right of the Canadian citizen to revoke his or her consent. Clause 4.3 requires that "knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."[123] The subsequent subclauses go into much greater detail regarding the time that consent should be obtained, and how consent can be obtained. Subclause 4.3.1 states that "an organization will seek consent for the use or disclosure of the information at the time of collection."[124] In addition, subclause 4.3.2 necessitates that "organizations shall make reasonable effort to ensure that the individual is advised of the purposes for which the

---

120 Id at 41.

121 Id.

122 Id.

123 Id at 39.

124 Id.

information will be used."[125] In order to ensure that consent is meaningful, "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed."[126] In other words, retailers and e-commerce companies should be upfront at the time of purchase the intent and reason for collection of the personal information. Finally, subclause 4.3.7 outlines multiple ways by which consent can be collected. Among these ways are a check off box, completion of an application form, or the time a consumer uses a service.[127] However, these are only examples, so Canadian law gives organizations and companies a great deal of leeway when deciding how they will obtain consent.

In 2012, the Australian Government passed the Privacy Amendment (Enhancing Privacy Protection) Act, which overhauled and amended the Privacy Act 1998. The legislation outlines thirteen Privacy Principles that companies must follow in order to stay compliant with Australian Privacy laws. The Privacy Amendment Act continuously refers to an APP entity. An APP entity is merely "an agency or organization."[128] Therefore, retailers should be very cognizant while reading through the thirteen principles that, while they are not based out of Australia, they are still considered an APP entity. Additionally, it is not necessary to discuss all thirteen as some of them do not apply to

---

125 Id at 40.

126 Id.

127 Id.

128 *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth) S 1.

non-Australian based companies, there are several that should be discussed, as they mirror what other countries. Among these Principles are the need for open and transparent management of information, what is required to collect certain information, an access requirement, and what can be collected by different companies. All of these topics are described in greater detail below.

Principle 1 of the Privacy Amendment requires that companies provide for open and transparent management of personal information. This principle requires that companies "have a clearly expressed and up-to-date policy (the APP Privacy Policy) about the management of personal information by the entity."[129] This privacy policy required by Subclause 1.3 should have the following seven points of information. A retailer or e-commerce company should ensure that their privacy policy contains:

> "(a) the kinds of personal information that the entity collects and holds; (b) how the entity collects and holds personal information; (c) the purposes for which the entity collects, holds, uses, and discloses personal information; (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information; (e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint; (f) whether the entity is likely to disclose personal information to overseas recipients; (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy."[130]

---

129 Id, pt 1 at 26.

130 Id.

All companies, regardless of their location, must ensure that they are notifying the consumer through this comprehensive privacy policy in order to be compliant with Australian law. Finally, companies must "take such steps as are reasonable in the circumstances to make its APP privacy: (a) free of charge; and (b) in such form as appropriate."[131] Principle 1 is a crucial portion of ensuring continuous compliance towards the Australian Privacy Amendment Act.

Principle 3 outlines the requirements for collection sensitive and non-sensitive personal information from consumers. Subclause 3.3(a)(ii) is of particular importance for retailers, as it states that "An APP entity must not collect sensitive information about an individual unless: (a) the individual consents to the collection of the information and;…(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities."[132] Principle 6 further touches on this notion of required consent, stating that if a retailer or e-commerce company "holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless: (a) the individual has consented to the use or disclosure of the information."[133] Similar to Canada, Australia has taken great strides in order to

---

131 Id, pt 1 at 27.

132 Id, pt 2 at 29.

133 Id, pt 3 at 32.

ensure that consent is a main requirement in ensuring that personally identifiable information is created and obtained through the consent of the consumer.

Finally, Australia has created multiple Principles surrounding the quality of personal information and the right of consumers to access that information. Principle 10 requires that retailers and e-commerce companies "take such steps (if any) as are reasonable in the circumstances that the personal information the entity collects is accurate, up-to-date, and complete."[134] Principle 11 requires that companies and retailers "take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified" in the event that the information collected is no longer required by the entity. Principle 12 requires that "if an APP entity holds personal information about an individual, the entity must, on request by the individual access to the information."[135] Finally, per Principle 13, companies and e-retailers must "take such steps (if any) as are reasonable to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant, and not misleading."[136] The new Australian law provides many rights and protections to the consumer to understand, consent to use, access, and correct any and all personal identifiable information provided to companies and e-commerce companies. The new law places the burden on the merchant to ensure they are

---

134 Id, pt 4 at 40.

135 Id, pt 5 at 41.

136 Id, pt 5 at 44.

transparent and open when obtaining and securing personally identifiable information provided by customers.

So How Do U.S. Companies Comply?

This analysis has so far walked through what can be and should be considered personally identifiable information and how a survey of countries and organizations (in the case of the European Union) seek to protect this information. The only thing left is to understand what companies should do in order to ensure that they are in compliance with the laws of various countries. While this question may seem troublesome to most retailers and e-commerce companies, since there are roughly 225 countries in the world, there are three basic areas companies should focus on when creating the internal legal framework to ensure they are in line with international law: compliance with the EU and Swiss Safe Harbor Rules, privacy policies and guidelines, and consent. Each of these areas has positives and negatives that will also be looked at in depth. Additionally, each of these topics overlap each other, as privacy policies and guidelines, as well as consent is addressed as part of the self-certification process for the U.S.-EU Safe Harbor regulations.

The first place retailers and e-commerce companies should look to when creating an international privacy infrastructure is to the US-EU Safe Harbor and the US-Swiss Safe Harbor Acts. Although Switzerland was not a focal country for this analysis, it is a good reference tool when trying to determine a comprehensive privacy compliance program. The US-EU Safe Harbor framework as developed as a result of the European

Commission's Directive on Data Protection, which went into effect in October of 1998.[137] As a result of the legislation, U.S. companies that were based outside the European Union, or were not found to meet the European Union's standard for privacy, would not be able to collect personal data from residents of the twenty-eight countries that belong to the European Union.[138] As a result, the U.S. Department of Commerce came together with the European Commission to create "Safe Harbor" framework.[139] Retailers and e-commerce companies that meet the threshold for adequacy can apply to the U.S.-EU Safe Harbor program. The same rationale influenced the United States to meet with Switzerland and create the same type of Safe Harbor for companies who meet the standards for Swiss privacy laws. The purpose of these Safe Harbor programs is to bridge the gap between the American legal policy regarding personally identifiable information and privacy and that of Europe. Europeans treat privacy as a fundamental right that should be controlled and monitored through legal means. American law takes the position that companies should take initiative and self-regulate the protection of personally identifiable information and that privacy.

The U.S.-EU Safe Harbor framework is composed of "7 privacy principles, 15 frequently asked questions and answers (FAQs), the European Commission's adequacy decision, the exchange of letters between the Department and the European Commission,

---

137 WELCOME TO THE U.S-EU & U.S.-SWISS SAFE HARBOR FRAMEWORKS, http://www.export.gov/safeharbor/index.asp, (last visited Apr. 10, 2015).

138 Id.

139 Id.

and letters from the Federal Trade Commission and the Department of Transportation on their enforcement powers."[140] This framework provides the guidelines and requirements for becoming a company that participates in the Safe Harbor program and how and where to provide the information required to self-certify. Retailers and e-commerce companies must submit to the Department of Commerce three pieces of information in order to self-certify.[141] First, a company must provide "the name of the organization, mailing address, email address, telephone and fax numbers."[142] Next, a company needs to provide a "description of the activities of the organization with respect to personal information received from the EU."[143] This requirement just requires the retailer or e-commerce company to declare what information they expect to receive from consumers in the EU in the normal course of business. Third, companies need to provide seven pieces of information regarding "the organization's privacy policy for such personal information."[144] Additionally, any company partaking in the Safe Harbor program must list on their privacy policy that "they adhere to the Safe Harbor Principles."[145] Finally, it

---

140 U.S.-EU SAFE HARBOR FRAMEWORK DOCUMENTS, http://www.export.gov/safeharbor/eu/eg_main_018493.asp, (last visited Apr. 10, 2015).

141 FAQ – SELF-CERTIFICATION, http://www.export.gov/safeharbor/eu/eg_main_018388.asp, (last visited Apr. 10, 2015).

142 Id.

143 Id.

144 Id.

145

should be noted that "the undertakings to adhere to the Safe Harbor Principles is not time-limited" and participating retailers and e-commerce companies should be ready to "apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the Safe Harbor for any reason."[146] The U.S.-Swiss Safe Harbor Framework is exactly the same as the U.S.-EU framework, except it applies solely for citizens of Switzerland. Therefore, if a retailer or e-ecommerce wanted to do business in Switzerland, and not the rest of the EU, they could apply solely to the U.S.-Swiss Safe Harbor Framework, and receive the same protections.

The downfall to the U.S.-EU Safe Harbor Provisions, and the U.S.-Swiss Safe Harbor provisions is based in the structure of the agreements. Particularly in that these Safe Harbors only protect organizations doing business with the twenty-eight member states of the European Union, or Switzerland specifically. However, most American retailers do not solely do business with such a small or select group of countries. Per Borderfree, a leader in international consumer driven e-commerce, notes that Canada is a leading market due to its relatively location to the United States and consumers comfort and familiarity with American retailers.[147] In fact, per their Borderfree Index (BFI), a "proprietary quantitative and qualitative measure to provide an indication of a market's relative cross-border ecommerce attractiveness. Canada scored five out of five possible

---

146 Id.

147 Id.

ONLINE SHOPPERS IN CANADA IDE3NTIFIED AS A TOP TARGET FOR U.S. RETAILERS, http://www.borderfree.com/press-events/online-shoppers-in-canada-identified-as-a-top-target-for-u.s.-retailers, (last visited Apr. 11, 2015).

'shopping carts' on the BFI, indicating that it is an "ideal market" for cross-border ecommerce."[148] So without Safe Harbor provisions, how do companies continue to comply with the privacy provisions in countries such as Canada and Australia, who are not a party to the Safe Harbor Acts?

The solution here is very simple. Companies should create a privacy policy that is compliant with both the Safe Harbor Framework, and the frameworks of all countries. Since the requirements for privacy policies vary from country to country, a company should do their due diligence in keeping their privacy policy as broad and as descriptive as possible during the creation, ensuring that all areas of privacy are covered. In order to understand what companies need to include in their privacy policy, they can start by looking at the US-EU Safe Harbor Framework and US-Swiss Safe Harbor Framework and the requirements for self-certification, as well as look into the laws of different countries to find out if there are any specific requirements, such is the case with Australia, that outline specific rights that consumers have to see and access their data.

First, companies can look to the various Safe Harbor Frameworks, which are conveniently identical in order to understand the very basics of what companies should provide in their privacy policies to obtain self-certification. There are seven basic principles that the self-certification process requires when describing what their privacy policy for personal information contains. The first necessitates that companies provide "where the privacy policy is available for viewing."[149] This component enforces that the

---

148 Id.

149

privacy policy be visible and available consumers for review at all time. To adequately protect themselves, companies should place their privacy policy in a visible place on their website. Additionally, companies may choose to place this in other places. For example, Borderfree, a leading global e-commerce provider, places a reminder on their checkout page which links the customer to their privacy policy, so consumers have a chance to click on it and read it prior to checking out.[150] Second, the Safe Harbor Framework requires companies to note the "effective date of implementation."[151] While this fact is important for self-certification, what is equally as important is noting the date of the updated privacy policy. As privacy laws, especially in the internet and e-commerce worlds continue to grow and change with the times, ensuring an up-to-date privacy policy is an important fact to protect companies from potential exposure or liability.

Third, companies must provide "contact office for the handling of complaints, access requests, and any other issues arising under the Safe Harbor."[152] This point is not just important for the compliance of Safe Harbor self-certification, but for proper notice in all privacy policies. For example, as seen in the previous sections, many countries require that consumers have access to their information upon request. Canada is an

---

 FAQ – SELF-CERTIFICATION, http://www.export.gov/safeharbor/eu/eg_main_018388.asp, (last visited Apr. 10, 2015).

150 MACY'S CHECKOUT PAGE, https://www.macys.com/chkout/internationalShipping, (last visited Apr. 11, 2015).

151 FAQ – SELF-CERTIFICATION, http://www.export.gov/safeharbor/eu/eg_main_018388.asp, (last visited Apr. 10, 2015).

152 Id.

excellent example, as their Personal Information Protection and Electronic Documents Act requires an Openness principle, in which "make readily available to individuals specific information about its policies and practices relating to the management of personal information."[153] In order to adequately protect itself from potential litigation or other legal issues, companies should always have a designated person or group to handle all privacy information complaints or requests for access to a consumer's personally identifiable information.

Fourth, retailers and e-commerce companies should provide "the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy." This clause does not mean that a specific body needs to be appointed, but just a jurisdiction or body of law by which all disputes will be managed and analyzed under. It is often easiest for companies to apply the laws and confirm jurisdiction under the guiding law of the jurisdiction in which the main headquarters is domiciled. For instance, Borderfree notes that "any disputes over privacy shall be governed exclusively by this privacy policy …including limitations on liability and exclusive application of the laws of and jurisdiction of the state of New York."[154] This puts consumers on notice of where and how all complaints regarding privacy policy violations will be settled or litigated.

---

153 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).

154 BORDERFREE PRIVACY POLICY, http://www.borderfree.com/privacy-policy, (last visited Apr. 11, 2015).

The fifth, sixth, and seventh principles will generally overlap for most retailers. The fifth principle requires companies to "name of any privacy programs in which the organization is a member."[155] The sixth principle states that companies provide a "method of verification" in order to show that organizations have a resource to investigate complaints of non-compliance of privacy standards.[156] Finally, the last principle necessitates companies have "the independent recourse mechanism that is available to investigate unresolved complaints."[157] Generally speaking, all of these tend to overlap by using an outside source for ensuring that the privacy standard is up to standard. Using Borderfree as an example, their privacy policy notes in several places their reliance on "TRUSTe's program requirements," which certify that they are compliant. In fact, the policy takes note that "privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability and choice regarding the collection and use of your personal information."[158] In conjunction, the policy notes that "if contacting us does not resolve your complaint, you may raise your complaint with TRUSTe."[159] These measures ensure

---

155 FAQ – SELF-CERTIFICATION, http://www.export.gov/safeharbor/eu/eg_main_018388.asp, (last visited Apr. 10, 2015).

156 Id.

157 Id.

158 BORDERFREE PRIVACY POLICY, http://www.borderfree.com/privacy-policy, (last visited Apr. 11, 2015).

159 Id.

that consumers know and understand they have outlets for voicing and obtaining resolution on any possible non-compliance to privacy laws, or inability to obtain their personally identifiable information.

In addition to these seven principles, retailers and e-commerce companies should post on their privacy policy and all Safeguards in which they are a part of. In fact, the US-EU Safe Harbor Framework and US-Swiss Safe Harbor Framework requires that companies "must also state in their relevant published privacy policy statements that they adhere to the Safe Harbor Principles."[160] This serves to put consumers on notice that they have gone through the process to prove they have done their due diligence to protect privacy laws. By including this disclaimer on their privacy policy, e-commerce companies and retailers are affirming that all of the following Safe Harbor Privacy Principles have been met. By meeting the following principles, retailers will cover and protect themselves against litigation or other legal action in almost all jurisdiction due to the broadness of the Principles.

First, it shows that the privacy policies put consumers on notice of "the purposes for which they collect and use information about them."[161] Companies are required to put consumers on notice of what information they are collect and for what purpose. By notifying customers, they are creating the opportunity for consumers to make an

---

160 FAQ – SELF-CERTIFICATION, http://www.export.gov/safeharbor/eu/eg_main_018388.asp, (last visited Apr. 10, 2015).

161 U.S-EU SAFE HARBOR OVERVIEW, http://www.export.gov/safeharbor/eu/eg_main_018476.asp, (last visited Apr. 11, 2015).

informed decision as to whether or not they want to provide this information. Secondly, companies must notify consumers of what is called "Onward Transfer, which is described as "Transfers to Third Parties." Companies should put consumers on notice that they intend to pass on their data to third parties and for what purpose, so consumers can make an informed decision if they want to pursue the transaction or purchase with the retailer or e-commerce merchant. Third, companies must notify consumers that they have "access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate."[162] This access is echoed in both the Canadian Personal Information Protection and Electronic Documents Act, and the Australian Privacy Amendment. For the Fourth Principle, companies must notify consumers that they have "reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction."[163] This notification of security and the different security measures to protect personally identifiable information conforms to all Privacy laws discussed in this analysis. Security is a uniform requirement that all Data Protection and Privacy Acts require. Under the Fifth Principle, the privacy policy should note the principle of data integrity, which requires that "personal information must be relevant for the purposes for which it is to be used."[164] Again, as previously noted in earlier analysis, this relevant and accurate requirement is stated in all Data Protection and Privacy Acts. The Sixth Principle of

---

162 Id.

163 Id.

164 Id.

enforcement, which provides recourse to ensure companies are complying with their own privacy policies was previously discussed in this section.

The final Principle coincides with the third thing retailers and e-commerce companies can do to protect themselves against violations of personal identifiable information protection. Choice is the final Principle that companies must comply with in order to be protected under the Safe Harbor Regulations. Choice denotes that retailers and ecommerce companies must give consumers the "opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected."[165] In other words, organizations must give consumers the opportunity to make an informed decision regarding the use of their personally identifiable information. This Principle is another way of saying that organizations must allow customers to consent to the use of their personally identifiable information, and that if a customer, making an informed decision, does not agree with the use, they must have the opportunity to rescind consent.

This coincides with every data protection and privacy protection law analyzed thus far. The concept of "consent" is explicitly mentioned in every piece of legislation promulgated by the six countries studied, and the European Union. In Directive 95/46/EC, the word consent is mentioned twelve times. More importantly, the Directive notes that where data is "capable by their nature of infringing fundamental freedoms or privacy" it is imperative that a "data subject gives his explicit consent."[166] The 2002

---

165 Id.

166

Directive references consent even more frequently than the 1995 Directive, using the term consent twenty-nine times. The Directive notes that a consumer may give consent "by any appropriate method of enabling a freely given specific and informed decision indication of the user's wishes, including by ticking a box when visiting an Internet website."[167] British, French, German, and Belgian data protection and privacy laws, as previously noted in Section 2, require an overt act in order to show that a consumer has given explicit consent to the use of their data for processing purposes. Canada goes a step further in terms of consent, nothing that companies cannot "require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes."[168] Finally, Australian Privacy Principle 3 requires that companies cannot collect personal data about a person unless the person "consents to the collection of the information and… if the entity is an organization – the information is reasonably necessary for one or more of the entity's functions or activities."[169]

It is clear through all the laws analyzed that explicit consent is required. This requirement forces companies to think through overt actions that consumers can take in order to show they consent. Implicit consent is not enough for these laws. In other words, it is not enough for companies to take data without a customer performing an act

---

 Council Directive 95/46/EC at 34.

167 Council Directive 2002/58/EC at 38.

168 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).

169 *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth) pt 1.

to show they understand what they are consenting to and providing that consent. For most companies, this can be fulfilled by having consumers click a box next to a disclaimer that they acknowledge a retailer or e-commerce company's privacy policy. For example, using the e-commerce giant Borderfree as an example, at the final checkout page, Borderfree notes that "By placing your order, you agree to the Terms & Conditions and Privacy Policy of Borderfree, macys.com's international fulfillment service."[170] Additionally, the company provides direct links to both their terms and conditions page, as well as their privacy policy in order to give consumers the chance to read them if they had not before. This is one of many examples that a company can mirror to show the consumer mad a concerted, overt effort to consent to the privacy principles of the company. By always relying on explicit consent and overt acts to show consent, retailers and e-commerce companies can protect themselves from potential lawsuits or other legal matters.

Conclusion

This paper sought to show what personally identifiable information is, how different countries regulate the collection and processing of personally identifiable information, and what U.S. retailers and e-commerce companies can do to protect against potential legal issues due to failure not to comply. While the cross-section of countries provided does not encompass a completely global perspective on the way countries

---

170 MACY'S CHECKOUT PAGE, https://www.macys.com/chkout/internationalShipping, (last visited Apr. 11, 2015).

protect personally identifiable information, there is enough information to understand the basic principles and create a sufficient protection against violations of privacy. As companies grow and expand, their understanding of how the different countries protect personally identifiable information should grow with it. However, if the three basic principles outlined in the third section are followed, particularly that of creating an extensive privacy policy and ensuring they have explicit and informed consent of the consumer, companies should remain adequately protected against lawsuits and potential litigation.