Ashley Green
Sensitive Information in a Wired World
Professor Joan Feigenbaum
Yale University
December 12, 2003

Over the past decade the world has gotten much smaller due to the electronic communication the Internet has fostered. While this promotes business and international relations, problems arise regarding the protection of individuals' personal information. Many countries around the world have developed privacy policies and laws protect an individual's information in the realm of electronic communication. Universal enforcement gets complicated because the Internet is not restricted to one country; it's worldwide. As a result, concerns arise regarding the compatibility of various countries' privacy policies. This paper will discuss the current legislation in place for various major countries[1], the existing conflicts between these countries' policies and the implications these conflicts hold for the protection of privacy on the Internet.

To begin, consider how countries handle the privacy of individuals in general, not exclusively in the electronic environment. Most countries around the world protect an individual's right to privacy in some respects, because "privacy is a fundamental human right that has become one of the most important human rights of the modern age"[2]. Definitions for privacy vary according to context and environment. For example, in the United States Justice Louis Brandeis defined privacy as the "right to be left alone"[3]. In the United Kingdom, privacy is "the right of an individual to be protected against

[1] Note: I restricted the study of international privacy laws only to countries who had similar government and social standards to the United States. Therefore, this study excludes many countries in Asia and Africa.

[2] Privacy and Human Rights 2003: Overview. <http://www.privacyinternational.org/survey/phr2003/overview.html > page 1.

intrusion into his personal life or affairs…by direct physical means or by publication of information"[4]. Australian legislation states that "privacy is a basic human right and the reasonable expectation of every person"[5]. Regardless of varying definitions of privacy, the importance of an individual's privacy is recognized on some level.

Every country in the world has a provision for privacy, even if it is as simple as the right to privacy in one's home or the right to secrecy of communication. On a more global level, international agreements such as the *International Covenant on Civil and Political Rights* and the *European Convention on Human Rights* protect the privacy of individuals around the world. We see that in order to protect the fundamental privacy rights of individuals, laws have been established on both local and global scales. Therefore, it follows that laws are also necessary to protect the information of individuals in the electronic environment.

Two types of laws are adopted by various countries to protect the sensitive information of individuals on the web. The first kind, comprehensive laws, are laws "that govern the collection, use and dissemination of personal information by both the public and private sectors"[6]. These general laws do not deal with individual areas like health care or educational systems. Instead, they establish standards for use of private information for all entities. Comprehensive laws are usually adopted for one of three reasons: to remedy past injustices, to promote electronic commerce or to ensure that laws are consistent with Pan-European laws[7]. In addition, comprehensive laws often require

---

[3] Privacy and Human Rights 2003: Overview 1.
[4] Privacy and Human Rights 2003: Overview 2.
[5] Privacy and Human Rights 2003: Overview 2.
[6] Privacy and Human Rights 2003: Overview 2.
[7] Privacy and Human Rights 2003: Overview 5.

the establishment of an independent commissioner to oversee the enforcement of the law. Unfortunately, problems arise because either a lack of resources hinders enforcement or the "independent" commissioner is under the control of the government[8]. The second set of laws are characterized as sectoral laws. These laws avoid broad, extensive legislation and instead target various sectors. The implied advantage of sectoral laws is their enforceability. Since they are so specific in nature, one would think that they would be easier to enforce than broad, comprehensive laws. On the other hand, introducing sectoral laws is a difficult because legislation has to be passed for each new sector[9]. While these two types of laws have their advantages and disadvantages, countries have formed a sharp divide by choosing one type of law or the other.

Comprehensive laws remain the main choice of many countries around the world. All countries in the European Union, Canada, Australia and the United Kingdom have chosen to implement legislation that is not sector specific. For example, the European Union adopted the *Privacy and Electronic Communications Directive* to prohibit the secondary use of all data without the informed consent of the individual[10]. Some of the details of this directive include the requirement of opt-in personally-identifiable online profiles, upfront notice when data is collected from data collectors[11] and the prohibition of data transference to any country that is not a member of the European Union. Although these details hold promising potential for privacy protection, they could present problems for European business. Specifically, the prohibition of data-transfer to countries other than those in the European Union hold implications for international business. How will

---

[8] Privacy and Human Rights 2003: Overview 7.
[9] Privacy and Human Rights 2003: Overview 3.
[10] Online Privacy: Promise or Peril. Lorrie Cranor. <http://lab.zoo.cs.yale.edu/cs156/lecture15.ppt> 28.

countries in the European Union be able to participate in international business with companies outside the EU if they can't transfer data? This question will be discussed lat I the paper.

Canada and Australia adopted a "co-regulatory" model of comprehensive laws. These co-regulatory laws allow the industry to develop and enforce rules for the protection of privacy, but a privacy agency (commissioner) oversees this enforcement[12]. Power is given to sectors to create and enforce industry specific laws, but a global agency still oversees the enforcement of these laws to ensure compliance. In addition, it is important to mention that both of these countries are members of the European Union and thereby abide by the standards adopted. For example, Canada set up the *Canadian Personal Information Protection and Electronic Documents Act*, which protects information transferred between the European Union and Canada.

The United Kingdom, like Canada and Australia, is also a member of the European Union and a supporter of comprehensive laws. In 1998, the UK approved the *Human Rights Act*, which incorporates the *European Convention on Human Rights* into domestic law[13]. The UK also established the *Data Protection Act of 1998* to "provide for limitations on the use of personal information, access to records and requires that entities that maintain records register with the Data Protection Commissioner"[14]. This act requires the establishment of a tribunal and the establishment of a commissioner to promote the appropriate usage of data by both government agencies and private entities[15].

---

[11] Privacy and Human Rights 2003: Overview 6.
[12] Privacy and Human Rights 2003: Overview 7.
[13] Privacy and Human Rights 2000: Country Reports. <http://www.privacyinternational.org/survey/phr2000/countriesru.html> page 19.

[14] Privacy and Human Rights 2000: Country Reports 19.
[15] Data Protection Act 1998. 16 July 1998. <http://www.legislation.hmso.

Specifically, the commissioner reports codes of practice to be laid annually before Parliament, assists in cases involving data processing and must comply with any decision made by the European Union[16]. Other details of this act include the individual's right to access personal data, to prevent processing and to demand the blocking, erasure or destruction of data by the entity in possession of this information[17].

Unlike the European Union, Canada, Australia and the UK, the United States has taken a different position regarding the establishment of privacy laws. There is no obvious right to privacy in the Constitution of the United States, but privacy is implied in a few of the provision in the Bill of Rights[18]. For example, American citizens have the right to "privacy from government surveillance into an area where a person has a reasonable expectation of privacy and also in matters relating to marriage, procreation, contraception, family relationships, child rearing and education"[19]. As a result, comprehensive privacy laws have not been adopted in the United States and instead, a network of sector-specific laws spans areas of personal information[20]. These sectors include, but are not limited to, financial reports, credit reports, health information and even video rentals. The main reason for these sectoral laws derive from the position taken by the White House and the private sector that "self-regulation is enough and that no new laws are needed"[21]. The United States believe that companies will voluntarily establish and monitor their own privacy practices, therefore removing the need for comprehensive privacy laws.

---

gov.uk/acts/acts1998/80029--a.html> page 4.
[16] Data Protection Act 1998 1.
[17] Data Protection Act 1998 1.
[18] Country Reports 21.
[19] Country Reports 21.
[20] Cranor 29.
[21] Country Reports 22.

The exception worth noting is the *Privacy Act of 2003* which gives consumers control over how their personal information is used, especially personal financial data, health data, driver's license information and social security numbers[22]. This act makes the misuse, purchase, sale or disclosure of an individuals social security number without the individual's permission illegal. The main purpose of this act is to "preempt identity theft (and other types of theft) by prohibiting the display and usage of social security numbers and their derivatives on federal documents (checks,Ids) also, by putting the responsibility on the commercial entities"[23]. This act appears sectoral in nature because it mainly deals with the use of social security numbers, but since this law applies to all commercial and governmental entities, it is more comprehensive than sectoral.

The different legal tactics adopted by the United States and the European Union and its member countries have created a significant theoretical conflict in the transfer of information between businesses and individuals in EU countries and the United States. The United States government recognized the misalignment in their sectoral laws and the comprehensive laws adopted by the European Union. As a result, the US lobbied the EU and its member countries to convince them that the privacy laws in the US were adequate[24]. Negotiations between the United States and the EU lasted for two years before an agreement was reached on July 26, 2000[25]. The negotiations resulted in the "safe harbor" agreement in which US companies had to agree voluntarily to a set of privacy rules created by the *US Department of Commerce* and the *Internal Market Directorate of the European Commission.* Sharp criticisms arose from privacy advocacy

---

[22] Privacy Act of 2003. Wesley C. Maness. 23 October 2003. <http://zoo.cs.yale.edu/classes/cs457/Wesley_Maness.ppt> slide 1.
[23] Wesley Maness slide 48.
[24] Privacy and Human Rights 2003: Overview 9.

groups on both sides because the agreement rests solely on the promises of US companies that they will not violate their declared privacy practices.

Despite the controversy, companies began to join the European Union Safe Harbor Privacy Program beginning with TRUSTe on November 1, 2000[26]. By July of 2003, roughly 350 companies based in the US had agreed to the Safe Harbor framework. The unimpressive number of companies that have agreed to adhere to "safe harbor" and the unfaltering international business relations, raises questions regarding the EU's enforcement of their strict privacy policies. If organizations in the EU follow the privacy policies then they would currently only be exchanging data with the 350 compliant US companies. If this is the case, then the incentive would exist for more companies to join safe harbor to maintain international business. But the numbers remain low and business has continued as usual, which implies that the companies in the European Union are still exchanging information with companies in the United States that are not members of safe harbor. Thus, this holds suspicious implications for the enforcement of the EU's privacy policies. Ironically, the "safe harbor" agreement is being re-evaluated this year[27].

Although conflicts have risen between the legal stance of the United States on privacy and other countries in the world, common ground does exist. Many countries, the United States and the EU included, are adopting Privacy Impact Assessments (PIAs). These PIAs are "assessments of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be

---

[25] Privacy and Human Rights 2003: Overview 9.
[26] TRUSTe Unveils European Union Safe Harbor Privacy Seal Program. Dave Steer. 1 November 2003. <http://www.truste.org/about/about_eu.html > page 1.
[27] Privacy and Human Rights 2003: Overview 10.

mitigated"[28]. In other words, considering and addressing privacy issues at the early stages of project implementation will reduce the chance that the project will have a negative impact on privacy after deployment[29]. Several requirements must be met for a PIA to be useful. First, the PIA process must be performed by an entity that is independent and not linked to either the government or the project being reviewed. Many countries, including Canada, the European Union and Australia, have set up commissioners to perform these duties.

Canada was the first government to make PIAs mandatory[30]. Canada's PIA "is responsible for ensuring that the federal government and companies in the private sector collect, use or disclose personal information in a manner that is responsible and transparent"[31]. The *European Union Data Protection Directive* requires all EU members' to implement a PIA and an independent privacy enforcement body. Also, the United States is in the process of creating and adopting a PIA. Until then, the US passed the *E-Government Act of 2003* to require federal agencies to conduct privacy impact assessments before developing information technology[32].

Given the conflicting privacy laws and common PIA policies instituted by Canada, Australia, countries in the European Union and the United States, several observations arise. First, it seems that too many mechanisms operate on a national level, rather than a global one. We see this in the conflict between the adoption of comprehensive laws vs. sectoral laws. Second, the use of self-regulatory devices for the

---

[28] Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners – Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online. Paige Anderson and Jim Dempsey. 1 May 2003.http://www.privacyinternational.org/survey/phr2002/ page 1.
[29] Privacy and E-Government 3.
[30] Privacy and E-Government 7.
[31] Privacy and E-Government 7.
[32] Privacy and E-Government 7.

protection of online privacy is inadequate. Laws, both national and global, are not going to be enough to protect an individual's privacy, because enforcement is difficult. Some countries, like the United States, rely on companies to self-regulate voluntarily. While other countries have put independent entities in place to enforce laws and oversee compliance, they often lack the motivation or resources to do so. More effective enforcement is needed through the implementation of technical solutions for privacy compliance and enforcement. Given the current legal climate for privacy protection, it is apparent that much more work needs to be done to protect the privacy of individuals in technological environments.

Works Cited

Data Protection Act 1998. 16 July 1998. <http://www.legislation.hmso.gov.uk/acts/acts1998/80029--a.html>

Online Privacy: Promise or Peril. Lorrie Cranor. <http://lab.zoo.cs.yale.edu/cs156/lecture15.ppt>

Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners – Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online. Paige Anderson and Jim Dempsey. 1 May 2003.<http://www.privacyinternational.org/survey/phr2002/>

Privacy and Human Rights 2000: Country Reports. <http://www.privacyinternational.org/survey/phr2000/countriesru.html>

Privacy and Human Rights 2003: Overview. <http://www.privacyinternational.org/survey/phr2003/overview.html>

Privacy Act of 2003. Wesley C. Maness. 23 October 2003. <http://zoo.cs.yale.edu/classes/cs457/Wesley_Maness.ppt>

TRUSTe Unveils European Union Safe Harbor Privacy Seal Program. Dave Steer. 1 November 2003. <http://www.truste.org/about/about_eu.html>.