The Protection of Privacy Rights in the United States

Edward C. Prado* & H. Tavish DeAtley**

In 1890, Samuel Warren and Louis Brandeis wrote, “Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the[] individual . . . , the right ‘to be let alone.’”1 When Warren and Brandeis wrote these words more than one hundred years ago, the threats to an individual’s privacy included “instantaneous photographs and newspaper enterprise(s).”2 Now, the primary threat is the Internet. Although the medium has changed, the concerns and ideological questions remain the same.3

Today, the right to privacy arises in many contexts as governments, corporations, and individuals attempt to define the boundaries of an individual’s privacy. These efforts make it clear that privacy is an evolving and contentious issue. The difficulty in defining and protecting privacy, it seems, stems directly from the constantly changing technological environment. Thus, any legal or practical principle that attempts to address privacy rights must be capable of adapting to the ever-changing landscape of our society. In the following discussion I will address current attempts to protect privacy rights in the United States. Additionally, I will discuss the enforcement mechanisms employed to protect privacy rights. Finally, I will analyze cross-border privacy protection.

---

2 Id.
I. United States Laws and Regulations


A. The Public Sector

The first type of legislation that Congress has employed to protect privacy rights includes acts that concern the disclosure and confidentiality of an individual’s government records. Two major pieces of legislation that exemplify this type of privacy protection are the Freedom of Information Act (“FOIA”) and the Privacy Act of 1974 (the “Privacy Act”). FOIA provides individuals access to government records so long as the information does not fall into one of nine exceptions.\footnote{Garcia, supra, note 4, at 698.} The Privacy Act outlines how governmental agencies control and disclose information regarding specific individuals.\footnote{Garcia, supra, note 4, at 698.}
These Acts strive to protect individuals from unnecessary governmental intrusions. The issue, however, is whether the legislation can remain effective and applicable as technology outpaces privacy laws.\(^\text{10}\)

Generally, the Acts have been successful. FOIA has been used to inform and educate the public by allowing the public to access government records. Any individual may ask for records, and the “burden falls on the government to sustain its decisions to refuse disclosure.”\(^\text{11}\) For the most part, FOIA emphasizes the importance of making the “fullest disclosure” possible.\(^\text{12}\) Any restrictions on disclosure are based on a delicate balancing of an individual’s right to privacy against the public’s right of access to government records.

While FOIA discloses government records regarding government action to the public, the Privacy Act limits the disclosure of government-held private information that pertains to individual citizens. Given our present concerns regarding the impact of technology on an individual’s privacy, the Privacy Act is of great relevance. The United States Privacy Protection Study Commission outlined the possible erosion of individual privacy rights due to the ease at which information can be accessed through advancing technology,\(^\text{13}\) and the Privacy Act, though it only addresses the governmental disclosure of information, still remains a vital tool in the battle to protect individual privacy rights.

\(^{10}\) Thomas Kearns, Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns, 7 WM. & MARY BILL RTS. J. 975, 1002 (1999).


\(^{12}\) Id.

B. The Private Sector

The second type of legislation that Congress has employed to protect privacy rights involves acts that limit access to an individual’s “personally identifiable information,” including financial information and Internet activity.\(^\text{14}\) There are four major pieces of legislation that illustrate this type of privacy protection: the Right to Financial Privacy Act (the “RFPA”), which prevents the government from accessing the financial records of individuals from financial institutions;\(^\text{15}\) the Electronic Communications Privacy Act (the “ECPA”), which precludes electronically-stored communication providers from disclosing any private information to the government;\(^\text{16}\) the Gramm-Leach-Bliley Financial Modernization Act of 1999 (the “GLBA”), which requires financial institutions to explain their information-sharing policies with consumers;\(^\text{17}\) and the Identity Theft and Assumption Deterrence Act (the “ITADA”), which criminalizes identify theft.\(^\text{18}\) Although these Acts were designed to prevent the disclosure of private material, they contain numerous loopholes.

Congress created the RFPA in response to the Supreme Court’s finding in *United States v. Miller* that an individual’s banking information was not considered private.\(^\text{19}\) However, as technology has eased the access to information, the RFPA has proven faulty. Specifically, the RFPA prevents the government from accessing an individual’s financial data, but it does not prevent “the financial institution from disclosing that information to a

\(^{14}\) Garcia, *supra* note 4, at 695.
fourth-party, who could then pass it on to the government.” This fourth-party loophole still remains open and is indicative of the difficulty of protecting privacy in the face of advancing technology. The ECPA is quite similar to the RFPA in that it limits disclosure to the government; however, the ECPA expands to include nondisclosure of all wired, electronic, and stored forms of communication. Even though the ECPA expanded its zone of privacy, it still includes the same fourth-party loophole as the RFPA.

The GLBA, while allowing for the consolidation of banks, securities, companies, and insurance firms, also requires financial institutions to address privacy concerns. It includes three main requirements: (1) companies must develop internal policies and structures to protect information, (2) notice must be given to consumers regarding the companies’ information-sharing policies, and (3) consumers must be given the ability to opt out of the information-sharing program. Although concerns exist as to whether an opt-out program is more effective and appropriate than an opt-in program, the GLBA represents a necessary step in protecting personal financial information.

The goal of the ITADA is to strengthen the protection of consumer personal information such as name, social security number, and credit card information. The ITADA’s main contribution to privacy protection is in its definition of identity theft. Prior to the ITADA, authorities could only prosecute an individual if that individual actually used the stolen information; however, under the ITADA, identify theft now includes the act of

---

21 Id. at 976–78.
23 See The Gramm Beach Bliley Act, supra note 22.
stealing the information. Additionally, for those convicted of identity theft, the ITADA includes harsher sentencing guidelines which have proven beneficial to the ITADA’s enforcement.

Although the ITADA has bolstered U.S. privacy protection, a tremendous amount of work remains to be done to counteract the role of the Internet in facilitating identity theft. The nature of privacy, its indefinite existence, and its lack of explicit constitutional protections make it difficult for laws to shield privacy rights from all angles. One example involves the difficulty of protecting private information from Internet electronic surveillance technologies such as “spyware” or “adware.” Spyware technology has the potential to perform a “wide range of undesirable activity . . . from outright theft of credit card numbers and other financially valuable data, to surveillance of every movement . . . consumers make on the Internet.” This is troubling on many levels, but it is especially disconcerting from the perspective of protecting individual privacy rights. Legislation is in place that criminalizes electronic surveillance and the theft of private information, but the original intent and understanding of the laws fail to consider spyware and adware. Thus, the laws, while clear in what they prevent, may allow such unwanted invasions of privacy.

Given the immense advancements in technology that we have seen in recent years, the United States has adapted quite well. However, it is evident that many attempts to protect privacy rights are simply

25 Id.
26 Spyware refers to software designed for the purpose of stealing information from one’s computer. Wayne Barnes, Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance, 39 U.C. DAVIS L. REV. 1545, 1547 (2006). Adware, although similar to spyware, is more benevolent as its purpose is to create advertisements that will “pop-up” on one’s computer. Id.
27 Id.
“patchwork[s] . . . designed to protect against disclosure.” These patchworks are capable of being successful, but only if the law stays current with new technologies.

C. Enforcement of Privacy Rights

It is generally understood that for a right to be protected, it must be rigorously enforced. “Absent an enforcement and redress mechanism,” statutes meant to protect privacy are “merely suggestive rather than prescriptive.” Currently, privacy rights are enforced in four ways: (1) federal action, (2) state action, (3) private remedies, and (4) business self-regulation.

With regard to federal action, the United States does not have an agency dedicated to the enforcement of privacy rights. However, the Federal Trade Commission (the “FTC”) has taken the lead in the federal effort to enforce privacy legislation. Draft legislation in the House of Representatives would grant the FTC more enforcement control, yet at this time, the FTC’s power is limited. Presently, the amount of enforcement depends on which act was violated and the extent of the violation. The ITADA permits convictions of up to fifteen years; however, it does not provide for restitution. Meanwhile, the GLBA provides no private right of action.

---

28 Simmons, supra note 20, at 976.
30 Id.
33 Draper, supra note 24, at 691.
34 Draper, supra note 24, at 691.
The second type of enforcement is through state action. Many states, in an effort to respond to public demand, have passed legislation that provides greater enforcement of privacy rights than that provided by the federal government. The State of California is a prime example: it has established an Office of Privacy Protection and is at the forefront of identity theft legislation. California’s main contribution to privacy protection has been its focus on the enforcement of privacy rights. Not only does California provide a simple means for individuals to freeze their credit/financial activity, it also has a streamlined process for reporting identity theft. Other regions, including the State of Minnesota and the District of Columbia, have passed statutes aimed at compensating victims of identity theft. In addition, the State of Nevada requires Internet providers to keep certain customer information private. These changes, though simple, represent marked improvements in the battle against identity theft.

The third form of enforcement is through private action. Because common law provides limited remedies, in most cases private rights of action depend on statutory schemes. For example, the ECPA “provides for civil damages, injunctive relief, and public equitable and criminal enforcement for violations.” However, private action is not a major avenue for enforcement because of the costs of litigation and the greater reliance on government led-enforcement. Furthermore, the lack of adequate

---

36 Id.
37 NEV. REV. STAT. § 205.498.
38 See, e.g., RESTATEMENT (SECOND) OF TORTS §652B (1977) (limiting the common law tort of intrusion upon seclusion to instances where the intrusion would be “highly offensive to a reasonable person”).
40 Id. at 907–08
compensation for violations of privacy rights creates a disincentive for individuals to seek enforcement.

II. Private-Sector Initiatives

The final avenue for enforcement is through institutional self-regulation; in other words, the private-sectors’ response to privacy issues that are complicated by the growth of its own technological offerings.41 The private-sector is forced to engage in a difficult balancing act: On the one scale, consumers appreciate and purchase technological innovations and want to share personal information with their friends and family using those new technologies. On the other scale, new technology users do not want to share the same personal information with every Internet user.

Additionally, the private-sector actively uses new technology to its advantage. It is well-established that potential employers use social networking sites and online searches to assess applicants.42 Unflattering photos, unfortunate comments, and acts we wish we could forget are all stored for posterity—and immediately accessible with a simple search—on the Internet.43

The phenomenal success of the social networking site, Facebook, now approaching 500 million users, is testament to the popularity of new technologies. However, Facebook itself demonstrates the dichotomy of consumer-interest and privacy protection. In late 2009, Facebook rolled out a series of changes to its privacy settings that allowed any Facebook user to see another user’s “friends” and collected information on whether a Facebook

---

43 Id.
user “liked” a third-party website. Facebook suffered a public relations backlash and succumbed to public pressure to change its privacy settings.

In another recent example, the effectiveness of privacy self-regulation was tested when Google launched a new email interface known as Google Buzz in February 2010. The software automatically made public the contact lists of the Buzz users. Users of Google revolted against the software and publically berated Google. Within days, Google had apologized and modified its privacy structure. Although some pointed to this as a “failure of privacy law in America, it would have been nearly impossible to conceptualize and design anticipatory legislation for the innovation behind Google Buzz.” Thus, a world of constantly advancing technology seems to lend itself to self-regulation.

Since the passing of the GLBA, companies have become more open to disclosing their information-sharing policies with consumers. Because of this, businesses have recognized the need to create formal policies that address consumer privacy concerns while at the same time ensuring that the policies are, in fact, enforced. Given the patchwork nature of legislation, self-regulation is an important additional means to protect privacy rights and allow for a “flexible market-driven approach” to remedying and preventing breaches of privacy.

However, the Facebook and Google Buzz examples produce an

---

46 Terenzi, supra note 41, at 1102–03.
47 Id.
48 Id.
49 Id.
50 See FED. TRADE COMM’N, Privacy Online: Fair Information Practice in the Electronic Marketplace: A report to Congress app. C, tbls. 1, 9a (May 2000) (finding that 68% of websites that collect personal information disclose their information-sharing practices)
important lesson: self-regulation by the private-sector is dictated by the whims of the public. Businesses make money using the information that individuals put on the Internet through highly-focused advertisements based on personal information. It is the responsibility of the consumer to push back against technological encroachment by purchasing from and using privacy conscious sites and selecting not to use sites that share information. Of course, at the most fundamental level, personal information protection starts with the individual technology consumer. There are many practices and precautions Internet users may avail themselves of to protect their information from disclosure or improper use.51

III. International & Cross-Border Issues

The Internet provides one with access to almost every corner of the world. Because of the Internet’s global reach, countries must consider the protection and enforcement of privacy rights on an international scale. The difficulty in formulating effective international policy lies in the differing views of privacy rights from country to country. The Organisation for Economic Cooperation and Development (“OECD”) released a report in 2006 that outlined the challenges in dealing with cross-border privacy law enforcement.52 In the report, the OECD explained that technical innovation has resulted in massive amounts of data being transferred across multiple borders before reaching their destinations. The resulting challenge is in “ensuring the protection of personal information when it crosses national borders.”53

53 Id.
Currently, the United States is engaged in an agreement with the European Union known as the United States-European Union Safe Harbor Agreement.\textsuperscript{54} The purpose of this agreement is to create a unified approach to privacy protection. This agreement requires countries and companies to follow seven principles: notice, choice, onward transfer, security, data integrity, access, and enforcement.\textsuperscript{55} Enforcement of these seven principles takes place through government or private means and in accordance with U.S. law.\textsuperscript{56} Additionally, the United States, in February 2010, participated in the formation of an international privacy initiative through the Asia-Pacific Economic Cooperation (“APEC”). The initiative, known as the APEC Cross-Border Privacy Enforcement Agreement (“CPEA”), is a voluntary agreement that provides a framework which allows for multilateral enforcement of privacy rights.\textsuperscript{57} The function of the CPEA is to ensure proper communication and cooperation between participating countries and institutions. At this point, only New Zealand, Australia, and the United States are participating, yet this agreement represents an important instrument through which privacy rights can be enforced internationally.

### IV. Conclusion

“Political, social, and economic changes entail the recognition of new rights . . . and the common law . . . grows to meet the demands of society.”\textsuperscript{58} The United States, for the past half century, has recognized and grown to meet society’s demand for a balancing of technology and privacy. As the

\textsuperscript{54} http://www.export.gov/safeharbor/ (last visited July 31, 2010).
\textsuperscript{56} Id.
\textsuperscript{58} Warren & Brandeis, supra note 1, at 193.
future brings new challenges, the law will be there to provide the patchwork necessary to continue protecting privacy rights.