PEPPERDINE UNIVERSITY

Journal of the National Association of Administrative Law Judiciary

Volume 32 | Issue 2 Article 10

10-15-2012

In the Middle: Creating a Middle Road Between U.S. and EU Data Protection Policies

Carolyn Hoang

In the Middle: Creating a Middle Road Between U.S. and EU Data Protection Policies

By Carolyn Hoang

TABLE OF CONTENTS

I. INTRODUCTION

His heart was steadily beating faster and his palms were beginning to sweat.[1] Even though he was an experienced highwayman, he never lost the nervousness that came right before he approached his victims. Perched atop his horse and shielded from view by the trees, he could see the coach approaching and could already tell that this meeting would yield enough to last him a month if he were to succeed. As the coach came around the bend, he took one quick breath, quickly pulled his mask over his face, and in one swift motion galloped forward from his hiding place amongst the trees to block the path. "Stop, and hand over your belongings!" he shouted, brandishing his pistol. The travelers, almost frozen in fear, slowly got out and emptied their pockets.

The above is a fictional account of a highway robbery during England's early days. Dating from the medieval times and into the nineteenth century, England's roads were ripe with highwaymen ready to take advantage of unsuspecting travelers.[2] In those days, robberies were much simpler—they occurred on the open highways and the victim knew exactly what was being taken. Today, in a world of free-flowing information and technology, things are much less simple. In an age in which intangible items, such as information, have as much value as tangible items, thieves have turned their focus from the real-world highway to the information highway.

The advent of technology and the Internet has brought unprecedented change to life as we know it.[3] Today, we

---

[1] This is an imagined account of a highway robbery in eighteenth century England. *See* Rictor Norton, *Highwaymen: Jack Hawkins, Sixteen-String Jack & Gentleman James Maclean*, THE GEORGIAN UNDERWORLD, http://rictornorton.co.uk/gu08.htm (last updated Jan. 28, 2012).

[2] *Highwaymen of the Peak*, BBC, http://www.bbc.co.uk/insideout/eastmidlands/series3/travellers_highwaymen_derbyshire_peakdistrict.shtml (last updated Mar. 2006).

[3] In response to predictions that "[c]ommerce and business will shift from offices and malls to networks and modems," author Clifford Stoll once commented: "Baloney. Do our computer pundits lack all common sense? The truth i[s] no online database will replace your daily newspaper . . . and no computer network will change the way government works." Clifford Stoll, *The Internet? Bah!*, NEWSWEEK (Feb. 26, 1995), *available at* http://www.thedailybeast.com/newsweek/1995/02/26/the-internet-bah.html. Time has proven these comments false.

communicate through the use of email and Skype; we buy products online; and we bank online.[4] The Internet has become a source that keeps us informed of current events, facilitates commercial transactions, and provides a means for social interaction. However, the Internet is a double-edged sword. Although it has made our lives easier in many respects, it has also created new problems. One of the merits of the Internet—the free flow of information—is also one of its greatest flaws. Anyone with the proper know-how can gain access to a user's most personal and valuable information.[5] In addition, these hackers can range from your average suburban kid to government agencies.[6] Unlike in the past, the things a person may

---

Indeed, few could have predicted the leaps and bounds that have been made by technology and the Internet. *See id*.

[4] Not only has the Internet changed our daily lives, it has also changed the way government works. Technology has forced government to work within the framework of the cyber world. Most notably, the Obama campaign in 2008 relied heavily on the Internet to reach out to voters. *See* Steve Schifferes, *Internet Key to Obama Victories*, BBC NEWS (June 12, 2008), http://news.bbc.co.uk/2/hi/7412045.stm; *See also* Claire Cain Miller, *How Obama's Internet Campaign Changed Politics*, NEW YORK TIMES BITS (Nov. 7, 2008, 7:49 PM), http://bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics/.

[5] Because of the nature of the Internet, it is impossible not to store any information about oneself online. Whether it be on a social networking site, on online banking, or on an Amazon account, each person has left some amount of personal information on the Internet. This, in turn, makes people more susceptible to identity theft. In fact, there is a huge market for stolen credit card numbers. Stolen cards, along with the names and addresses on the card, are sold on forums for those who know where to look and are sold for about five to ten dollars apiece. *See* Nick Bilton, *How Credit Card Data Is Stolen and Sold*, NEW YORK TIMES (May 3, 2011, 3:30 P.M.), http://bits.blogs.nytimes.com/2011/05/03/card-data-is-stolen-and-sold/.

[6] Early in 2012, it was reported that a group of high school juniors in southern California had hacked into their teacher's computers in order to change the grades of students who were willing to pay for their "services." *See* Dennis Romero, *Rich Kids Hack Computers to Change Grades at Palos Verdes High but are Busted by Cops*, L.A. WEEKLY BLOGS (Jan. 27, 2012, 12:32 PM), http://blogs.laweekly.com/informer/2012/01/palos_verdes_grade_change_computer_scandal_high_school.php.

In contrast, some hackers operate for the government and gather information as intelligence. *See* Tabassum Zakaria, *U.S. Blames China, Russia for Cyber Espionage*, REUTERS (Nov. 3, 2011), http://www.reuters.com/article/2011/11/03/us-usa-cyber-china-

own today are not only limited to physical forms. In this technological age, a person's possessions may also take on a digital form; and with this transition from the physical to the digital has come a stealthier form of theft that is much different from face-to-face hold-ups. Unlike the days of yore, the online security breaches of the modern age happen right under the victim's nose without her knowledge, and it is often difficult to realize the full extent of the harm until much, much later.[7]

With the pattern of current events, it is even more difficult to ignore the growing problem of security breaches. A security breach that has recently garnered much attention in the press is the hacker group Anonymous's breach into think-tank Stratfor's database.[8] The hacking group was able to obtain the email addresses and other personal data of Stratfor's 860,000 subscribers, which included high-profile government officials.[9] The result was not only a nightmare for the subscribers, but for the United States as well, with an analyst for independent research institute, U.S. Cyber Consequences Unit, John Bumgarner stating, "[w]e can assume that a foreign intelligence service has already taken advantage of this information."[10] To add insult to injury, it was later discovered that Stratfor's data protection

---

idUSTRE7A23FX20111103. In 2011, the U.S. accused China and Russia of engaging in cyber espionage. *Id.* It is believed that foreign countries target the U.S. for trade secrets in order to gain "parity with the United States" *Id.* National Counterintelligence Executive, Robert Bryant emphasized the danger it posed to the U.S., stating: "Trade secrets developed over thousands of working hours by our brightest minds are stolen in a split second and transferred to our competitors." *Id.*

[7] *American Greed: Cybercrime* (CNBC television broadcast May 5, 2010), *available at* https://www.youtube.com/watch?v=LTVJ9rpwiFQ (Starting at 17:39, Julie, a victim of stolen credit card information describes the effect it has had on her life. She has had to spend countless hours resolving problems arising from theft of her information.). *See also* Nicole Perlroth, *Finding a Cleanup Crew After a Messy Hack Attack*, NEW YORK TIMES (Dec. 29, 2011), http://www.nytimes.com/2011/12/30/technology/hacker-attacks-like-stratfors-require-fast-response.html ("In the world of computer security, experts say, the most dangerous breaches are the quiet ones—the ones in which hackers make off with a company's intellectual property and leave no trace.").

[8] *See* Ken Dilanian, *Hackers Reveal Personal Data of 860,000 Stratfor subscribers*, LOS ANGELES TIMES (Jan. 4, 2012), http://articles.latimes.com/2012/jan/04/nation/la-na-cyber-theft-20120104.

[9] *Id.*

[10] *Id.*

left much to be desired. The company's files were unencrypted,[11] and an individual was able to crack user's passwords using simple off-the-shelf software.[12] Due to its faulty data protection, Stratfor lost highly confidential information that was costly to both its consumers and the country.

This example of a security breach serves as a testament to the far-reaching consequences of poor data protection. If a system does not have adequate data protection, it can easily be hacked. Then, the hacker will gain access to information belonging to multitudes of people, agencies, and groups. These recent developments beg the question: What does this mean for the future of America's data protection practices? Should the government play a role in regulating data protection to ensure that its citizens' data are adequately protected?

The current framework for U.S. data protection is based upon a "sectoral model" in which various laws aimed at different sectors of industry are used to protect personal information. This model relies upon a combination of legislation, regulation, and self-regulation in order to protect data privacy.[13] In practice, this is how the sectoral model works: Congress passes legislation and, through the Federal Trade Commission and the Department of Commerce, monitors the businesses targeted by the legislation. However, these laws are narrow in scope and are careful not to infringe too much on the marketplace's role in privacy regulation.[14] While the model does include the use of legislation, it primarily relies upon industry practice, codes of conduct, and the marketplace in order to protect data privacy.[15] Reliance on legislation to provide data protection is secondary to reliance on industry practice to protect data.[16] The rationale is that businesses are in the best position to make data

---

[11] Zoe Fox, *'Anonymous' Hackers Hit Security Group*, CNN (Dec. 26, 2011), http://www.cnn.com/2011/12/26/tech/web/anonymous-hack-stratfor/index.html. It appears that Anonymous targeted Stratfor because it failed to encrypt credit card data of its clients. *Id.*

[12] Dilanian, *supra* note 8.

[13] *See U.S.-E.U. Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 26, 2012).

[14] *Id.*

[15] *Id.*

[16] *Id.*

privacy decisions that will suit both their needs and the needs of the consumer.

Although the U.S.'s sectoral model gives businesses freer rein in its data collection practices by allowing businesses to pick and choose how to implement privacy protection laws, some have wondered whether the sectoral model is the better model or whether it is even effective at all.[17] With online privacy becoming an increasingly hot topic,[18] many are pondering whether it is time for the U.S. to have its own data protection agency.[19] Those who call for change point to the European Union (EU) and its approach to data privacy, which is considered to be the most stringent in the world. Unlike the U.S.'s sectoral model, the EU's comprehensive model creates expansive political rights to citizens of member states and gives control of personal information to the citizen.[20] In this way, the EU model is the exact opposite of the U.S. model of data protection in that the latter takes control of personal information away from the consumer and puts it in the hands of businesses.[21]

---

[17] *See* Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1192 (1999).

[18] Most notably, Facebook has recently been under fire for tracking and keeping logs of sites that its users visit. *See* Tiffany McCall, *Facebook Privacy Concerns,* WKRG-NEWS (Nov. 17, 2011), http://www2.wkrg.com/news/2011/nov/17/facebook-privacy-concerns-ar-2719783/. Even more recently is the hacking of security group, Stratfor's client information. *See* Zoe Fox, *'Anonymous' Hackers Hit Security Group*, CNN (Dec. 26, 2011), http://www.cnn.com/2011/12/26/tech/web/anonymous-hack-stratfor/index.html.

[19] *See generally* DEPARTMENT OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY (2010), *available at* http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf [hereinafter DEPARTMENT OF COMMERCE] (In this paper, the Department of Commerce proposed a creation of an online data protection agency).

[20] James M. Assey & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMM. LAW CONSPECTUS 150 (2001).

[21] Fred H. Cates, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 207–08 (1999) ("[I]n the United States, telephone numbers, addresses, Social Security numbers, medical history, and similar personal identifying data are almost always owned by someone else—the Post Office, the government, or a physician or hospital.").

States within the EU provide their citizens with strong data privacy rights.[22] In fact, data protection is considered a fundamental right guaranteed to all citizens within the EU states under a law called Directive 95/46/EC (Directive) that was passed in 1998.[23] The Directive also requires companies to obtain consent from consumers before collecting, processing, and sharing personal information.[24] Further, this EU law allows consumers access to their information in order to update and change it.[25] Essentially, the Directive works to protect personal data by giving the individual a great deal of control over her personal information. Lastly, the Directive also works to provide security by controlling the parties with which an EU company may trade.[26] The Directive only allows for transmission of data between an EU member and a non-EU party if the party has "adequate" data protection.[27] This requirement is meant to ensure that data will not be transmitted to a party that will be careless with the information.[28] The basis of the EU model is the idea that data

---

[22] *See* Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Art. 28. 1995 O.J. (L 281) (Oct. 24, 1995), *available at* http://www.unhcr.org/refworld/docid/3ddcc1c74.html [hereinafter Data Directive].

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *See* Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995 O.J. (L 281).

[28] *See id.* When the Directive was first passed, many, especially the U.S., were in an uproar. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS 191–95 (1998). The restriction on transmission of data between an EU country and a non-EU country had significant economic consequences, specifically for those in the financial industry. *Id.* at 34. Many in the U.S. were afraid that the EU had created this restriction in order to discriminate against foreign trading partners, but this matter soon blew over with the Safe Harbor Agreement in 2000. *See id*. at 191–95; *see also Safe Harbor*, EXPORT.GOV (Apr. 11, 2012), http://export.gov/safeharbor/.

The Safe Harbor Agreement allowed flow of information between the EU nations and the U.S. so long as U.S. businesses complied with the requirements set out in the agreement. In order to qualify for Safe Harbor and trade with a business located in the EU, a U.S. company must fill out a form on the U.S. Department of Commerce's website and certify that the requirements under the Safe Harbor agreement are met. *See* Eric Shapiro, *All is Not Fair in the Privacy Trade: The*

privacy is a "political right anchored among the panoply of fundamental human rights and the rights attributed to 'data subjects' or citizens."[29]

The EU Directive sets up the foundation of EU data privacy protection, but the way the Directive is enforced depends on the member state and how it chooses to administer the law. Each state is given the freedom to decide how it will run its independent agency in charge of ensuring that data protection policies are being followed and which laws must be passed in order for it to comply with the spirit of the Directive. This type of freedom creates differences among the privacy policy regime that each State enacts. For instance, France's independent agency is chaired by members who hold additional positions in the federal government while the United Kingdom's independent agency is chaired by members who do not hold additional positions within government.

This paper seeks to explore the question of how much we should borrow from the EU model of data protection. In order to determine whether the EU's system is appropriate for the U.S. to imitate, it is helpful first to examine the Directive, and second to analyze its implementation by EU member states. The two EU member states that will be examined are the U.K. and France. These two countries were chosen as part of the analysis because of their unique and different approaches to the Directive's implementation. Most importantly, both countries approach data protection using different levels of government interference and have defined government regulation in contrasting ways. In order to truly understand the options available to the U.S. if it were to implement the EU approach, it is important to see how the EU states, themselves, have implemented the approach.

The first section of this paper will examine the historical differences that have led to the American approach to privacy and the European approach to privacy. The second section will examine the current U.S. model, and the third section will examine the EU model. Next, the fourth section will compare and contrast the two models.

Safe Harbor Agreement and the World Trade Organization, 71 FORDHAM L. REV. 2781, 2786 (2003) (arguing that the Safe Harbor Agreement has a very lax standard that does not ask much of U.S. companies).

[29] Assey & Eleftheriou, *supra* note 20, at 145, 148.

Finally, the last section will argue that the U.S. should have a regulatory agency and describe how that should look and run.

II. EXISTING U.S. MODEL

The current U.S. sectoral model of data protection was also greatly influenced by the Clinton administration.[30] The rationale was that it would be better for businesses to regulate themselves than to have government intervene.[31] Although businesses would be regulated by *some* laws, for the most part, businesses would decide how to implement data protection. Indeed, state and federal regulatory laws are only one component of the U.S. informational privacy policy. Even so, they are important nevertheless, because they define the scope and dictate the areas in which data privacy may be enforced.

Currently, U.S. data privacy protection consists of a hodgepodge of laws that were originally drafted for the government and specific sectors of the economy. Most of these laws were not created to apply to information gathered online, but over time they have been used to regulate data privacy. Aside from legislation, recent developments in case law are also beginning to shape data protection.[32] Unlike the EU model, where data privacy is a protected right, U.S. data privacy law is founded on tort and contract principles.[33] Although these laws borrow from various legal areas

---

[30] See WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 1–2 (1997), *available at* http://www.w3.org/TR/NOTE-framework-970706.

[31] *Id.*

[32] *See* Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007); Guin v. Brazos Higher Educ. Serv., Civ. No. 05-668, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006); Bell v. Mich. Council, 2005 Mich. App. LEXIS 353 (Mich. App. Feb. 15, 2005).

[33] *See* Thomas J. Smedinghoff, *Defining the Legal Standard for Information Security*, *in* SECURING PRIVACY IN THE INTERNET AGE 19, 22 (Anupham Chander, et al. eds., 2008) (noting that recent case law has upheld that breach of the common law duty to provide security amounts to a tort); Jonathan K. Sobel et al., *The Evolution of Data Protection as a Privacy Concern, and the Contract Law Dynamics Underlying It*, *in* SECURING PRIVACY IN THE INTERNET AGE 55, 57–59 (Anupham Chander, et al. eds., 2008) (arguing that federal data protection laws are based on contract principles).

and apply to different sectors, it has been argued that these laws are "amazingly consistent in [their] approach . . . ."[34] In his article, *Defining the Standard for Information Security*, Thomas J. Smedinghoff argues that laws concerning information security have been consistent in defining the legal standard for data protection.[35] Smedinghoff argues that each law has approached data protection with the idea that "Security is a process, not a product."[36] Thus, these laws do not rigidly dictate the requirements for "reasonable security."[37] Rather, Smedinghoff identifies that data protection laws have set a "process oriented" legal standard, meaning that they "[focus] on a process to identify and implement measures that are reasonable under the circumstances to achieve the desired security objectives."[38] Indeed, when the federal laws are examined later in this article, we will see an unmistakable pattern of assessment of risk, identification of security measures, and verification of implementation that is required by the "process oriented" standard.[39]

So, despite the fact that there are multiple areas and types of information being regulated on both state and federal levels, it seems that the laws do follow a consistent standard. Currently, there are a slew of different federal laws. Some apply only to the government's collection and use of personal information, while others apply to specific sectors of industry and still others apply to protect certain portions of the population.

A. Data Privacy Laws at the Federal Level

At the federal level, laws that protect citizens against the government's use of personal information are the Privacy Act of 1974[40] and the Freedom of Information Act (FOIA).[41] The Privacy Act of 1974 states that any federal agency collecting personal information for government records must: (1) collect only personal

[34] *See* Smedinghoff, *supra* note 33, at 23.
[35] *Id.*
[36] *Id.*
[37] *Id.* at 23–24.
[38] *Id.* at 24.
[39] Smedinghoff, *supra* note 33, at 24.
[40] 5 U.S.C. § 552a(e)(1)–(5) (2006).
[41] 5 U.S.C. § 552 (2006).

information that is "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President"; (2) maintain the accuracy of the information, and; (3) establish means of protecting the security of the information.[42]

Similarly, FOIA makes the government responsible for guarding the personal information found in federal agency records.[43] Although FOIA is a law ensuring public access to governmental records, the Act protects privacy by exempting the public from obtaining personnel, medical, and law enforcement records.[44] Although these statutes were designed to apply primarily to federal records and government, they are not limited only to information gathered in the real world; thus, they may be applied to information gathered online as well.[45]

Congress has regulated businesses' data collection and use by enacting laws aimed at specific sectors of the market as well as specific sections of the population.[46] These laws have been passed one at a time, and government regulation is beginning to expand to cover just about every possible sector. Laws governing the business sectors are: the Fair Credit Reporting Act (FCRA),[47] the Cable Communications Policy Act (CCPA),[48] the Health Insurance Portability and Accountability Act (HIPAA),[49] the Children's Online Privacy Act,[50] the Gramm-Leach-Bliley Act (GLBA),[51] the

---

[42] *See* 5 U.S.C. § 552a(e)(1), (5), (10).

[43] *See* 5 U.S.C. § 552.

[44] *See id.*

[45] *See id.* § 552(a)(3)(C) ("[A]n agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.").

[46] *See* Sobel et al., *supra* note 33, at 59.

[47] 15 U.S.C. §§ 1681–1681x (2006).

[48] 47 U.S.C. §§ 521–554 (2006).

[49] 42 U.S.C. § 1301 (2006).

[50] 15 U.S.C. § 6501 (2006).

[51] 15 U.S.C. §§ 6801–6809 (2006).

Sarbanes-Oxley Act,[52] and the Federal Trade Commission Act, section 5 (FTC Act).[53]

1. Fair Credit Reporting Act

Enacted in 1970,[54] the FCRA was the first federal law intended to regulate private businesses' use of personal information, especially where the consent of the individual has not been obtained.[55] This Act is especially important to the U.S. system of data protection because it provides the basis for the country's modern-day privacy legislation of "notice–and–consent" and "access to information."[56] The FCRA allows a credit agency to distribute a credit report containing personal information in order to determine the individual's eligibility for credit, insurance, employment, and the like, but the act requires the credit agency to take reasonable measures to ensure the accuracy, relevancy, and proper use of the information.[57] The FCRA regulates traditional as well as online credit reporting activities.[58] Some have noted that the FCRA approaches data privacy using a "pseudo-contractual" approach to data protection by allowing customers to change the scope of their relationship with credit reporting agencies.[59]

2. Cable Communications Policy Act

In 1984, Congress passed the CCPA,[60] which requires cable companies to provide their customers with annual notice as to how their information is being used and the purpose for which it is being used.[61] The CCPA also requires cable companies to give their

---

[52] Pub. L. No. 107-204 § 304 (2002).

[53] 15 U.S.C. § 45(a)(1) (2006).

[54] *The Fair Credit Reporting Act, (FCRA) and the Privacy of Your Credit Report*, EPIC.ORG, http://epic.org/privacy/fcra/ (last visited Nov. 19, 2012).

[55] 15 U.S.C. §§ 1681-1681x. *See also* Sobel et al., *supra* note 33, at 60.

[56] Sobel et al., *supra* note 33, at 60.

[57] *Id.*

[58] *Id.*

[59] *Id.* at 58.

[60] Cable Communications Policy of 1984, 47 U.S.C. §§ 521–554 (2006).

[61] *Id.*

customers the option to remove their name from any mailing list before the list may be released to a third party.[62]

3. Health Insurance Portability and Accountability Act

HIPAA was passed in 1996, and like the data protection laws before it, HIPAA requires medical providers, insurers, and other entities handling health information to adopt a system for notice, opt-out-disclosures, and access to private information.[63] The Act also requires secure transmission of health data.[64]

4. Gramm-Leach-Bliley Act

The GLBA, also known as the Financial Modernization Act of 1999, adds onto the provisions of the FCRA. The GLBA requires financial institutions to provide customers with notice of its information sharing practices along with an opportunity to opt out of certain disclosures of personal information to third parties.[65] The GLBA also prohibits financial institutions from disclosing account numbers to unaffiliated third parties.[66] Further, the Act not only puts responsibility on companies, but also on the FTC by requiring that the Commission formulate a Safeguards Rule that businesses must follow.[67]

5. Federal Trade Commission Act Section

Lastly, section 5 of the FTC Act is also employed to ensure data privacy. Although the Act, passed in 1938 and amended in 1994, has long been present in consumer protection jurisprudence, it has only recently been applied to information security.[68] Essentially, section 5 is a catch-all that regulates the business sectors that have

---

[62] *Id.*

[63] Sobel et al., *supra* note 33, at 58.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] 16 C.F.R. § 314 (2012).

[68] Smedinghoff, *supra* note 33, at 22. Section 5 was first applied to information security in 2005. *Id.*

not been covered by federal regulation. The FTC has asserted that "failure to provide appropriate information security was itself, an unfair trade practice . . . ."[69]

Section 5 has been used to halt a number of practices dangerous to information privacy. First, it can be used to protect consumer data. In a complaint brought by the FTC against DSW, Inc., the FTC charged the company with engaging in an unfair practice when it allowed hackers to gain access to the credit card and checking account numbers of over 1.4 million customers.[70] The FTC stated that DSW "failed to provide reasonable and appropriate security for sensitive customer information."[71] DSW had stored sensitive information in multiple files when it no longer needed such information, failed to use "readily available security measures," and stored information in unencrypted files, among other things.[72] Second, the FTC has also applied section 5 to "phishing."[73] In 2004, the FTC brought a complaint against Zachary Hill for engaging in phishing activities.[74] Hill had sent fraudulent emails to AOL users asking for users' passwords and login names along with their bank account numbers and Social Security numbers.[75] Third, the FTC has also applied section 5 to operations that secretly download spyware onto a user's computer. In a complaint brought against Seismic

---

[69] *Id.*

[70] *DSW Inc. Settles FTC Charges*, FEDERAL TRADE COMMISSION (Dec. 1, 2005), http://www.ftc.gov/opa/2005/12/dsw.shtm.

[71] *Id.*

[72] *Id.*

[73] Phishing is a form of identity theft. Con artists set up fake websites or send fraudulent emails that gather a user's personal information, such as passwords and credit card information, once a user visits the website or opens the email. *See Phishing: Frequently Asked Questions*, MICROSOFT SAFETY AND SECURITY CENTER, http://www.microsoft.com/security/online-privacy/phishing-faq.aspx (click "What Is Phishing") (last visited Dec. 30, 2012).

[74] *See FTC, Justice Department Halt Identity Theft Scam*, FEDERAL TRADE COMMISSION (Mar. 22, 2004), http://www.ftc.gov/opa/2004/03/phishinghilljoint.shtm. The Department of Justice eventually secured a 46-month prison sentence against Hill. *See* FTC v. Hill, H 03-5537 (E.D. Va.), *available at* http://www.ftc.gov/os/caselist/0323102/0323102zkhill.shtm (click on "Criminal Information").

[75] *FTC, Justice Department Halt Identity Theft Scam,* FEDERAL TRADE COMMISSION, *supra* note 74.

Entertainment Productions, the FTC argued that Seismic engaged in unfair acts and practices when they downloaded software without notifying users.[76] Seismic had downloaded spyware onto users' computers which then compelled users to purchase "Spy Wiper" in order to have the spyware programs deleted.[77] The FTC noted that it was an unfair act to "compel" users to purchase Spy Wiper by compromising their computers.[78] But the FTC also found the act of installing the spyware, in the first place, as an unfair practice in and of itself because it was done without the user's knowledge or permission.[79]

6. Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA), enacted in 1998, is unlike most data protection laws in that it was aimed at protecting a specific section of the population rather than regulating a specific market.[80] COPPA was aimed at regulating the collection of information of children under the age of thirteen.[81] Indeed, it requires web operators to comply with notice requirements and obtain parental permission before disclosing a child's personal information.[82] Again, we see contract principles coming into play—here, minors are not able to contract and thus parents must make the decisions for them.

---

[76] *FTC Cracks Down on Spyware Operation,* FEDERAL TRADE COMMISSION (Oct. 12, 2004), http://www.ftc.gov/opa/2004/10/spyware.shtm.

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *See* COPPA, *Children's Online Privacy Protection Act*, COPPA, http://www.coppa.org/comply.htm (last visited Oct. 12, 2011).

[81] *Id.*

[82] COPPA poses a big problem to social networking websites such as Facebook. *See* Emily Bazelon, *Why Facebook Is After Your Kids*, NEW YORK TIMES (Oct. 12, 2011), http://www.nytimes.com/2011/10/16/magazine/why-facebook-is-after-your-kids.html?_r=0. This also raises the question of enforcement of COPPA on such websites—who is to stop a 12 year old from creating an account on Facebook?

B. State Laws

In addition to federal laws, there are state laws that govern privacy protection. Virtually all states have laws requiring a business to notify a consumer when its security has been breached.[83] Other states have gone farther and have also enacted data destruction laws, or laws requiring the destruction of data once the business no longer wants to retain the information.[84] In addition, some states also have laws imposing a duty on a business to provide security for personal information.[85] State regulation in this area has been a relatively new occurrence. When California passed its security breach notification law in 2003, it was the first state to do so and the legislation was considered a "landmark."[86] Since then, other states have followed and are moving towards the trend of broadening data protection.[87] It

---

[83] Smedinghoff, *supra* note 33. *See also* CAL. CIV. CODE § 1798.82 (2007) (" Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident . . . . "). *Id.* § 1798.82(a).

[84] *See* CAL. CIV. CODE § 1798.81 (West 2012). States that have similar laws are: Arkansas, Connecticut, Georgia, Hawaii, Illinois, Indiana, Kentucky, Maryland, Massachusetts, Michigan, Montana, Nevada, New Jersey, North Carolina, Oregon, Texas, Utah, Vermont, and Washington. *See also* Smedinghoff, *supra* note 33, at 33.

[85] These states include: Arkansas, California, Connecticut, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah. Smedinghoff, *supra* note 33, at 32.

[86] *See* Privacy Rights Clearinghouse, *Fact Sheet 17b: How to Deal With a Security Breach*, PRIVACY RIGHTS CLEARINGHOUSE, (Feb. 2006), https://www.privacyrights.org/fs/fs17b-SecurityBreach.htm. *See also* Alexander P. Woollcott, *California Significantly Expands Privacy Breach Notification Law*, MMM TECH LAW & BUSINESS REPORT, http://www.mmmtechlaw.com/2011/09/22/california-significantly-expands-privacy-breach-notification-law/ (last visited Dec. 30, 2012).

[87] *See* Woollcott, *supra* note 86. *See also Massachusetts Privacy Law – 201 CMR 17 Compliance*, RAPID 7, http://www.rapid7.com/solutions/compliance/mass-201-CMR-17.jsp (last visited Dec. 30, 2012) (noting that Massachusetts's new data privacy law has "set a new level in state security laws . . . . " The law was unlike the laws before it in that it applied to private and public sector entities "regardless of where that entity is located.").

is interesting to note that some of the laws incorporate federal laws. For instance, California's privacy breach notification law was expanded in 2011 to provide that entities that are subject to HIPAA will be considered as in compliance with the privacy breach notification law if those entities have complied with breach notifications under HIPAA.[88] In addition, Massachusetts passed 201 CMR 17 in 2008, a law that incorporated the Gramm-Leach-Bliley Act.[89]

C. Enforcement

The FTC and the Department of Commerce are assigned the task of fulfilling the "regulating" part of the sectoral model. In addition to its main task of investigating and reporting to Congress foreign trade conditions and domestic business conduct, the FTC regulates online privacy to the extent that it relates to business and trade. Unfortunately, the FTC is limited in that it does not have the independent power to enforce data protection and there must exist a rule of law before it can do so.[90] This means that the FTC cannot prevent data collection and distribution unless the collector has posted a privacy policy and then failed to act in accordance to that policy.[91]

The Department of Commerce also plays a role in regulating data protection and has several agencies that help it do so: the National Telecommunications and Information Administration (NTIA), the International Trade Administration (ITA), the National Institute of Standards and Technology (NIST), and the Internet Policy Task Force.[92] It is important to note, however, that these

---

[88] *See* Woollcott, *supra* note 86.

[89] *Massachusetts Privacy Law – 201 CMR 17 Compliance*, RAPID 7, *supra* note 87; JILL JUDD, MA 201 CMR 17 STANDARDS 1 (2009), *available at* http://www.whipplehill.com/ftpimages/408/misc/misc_63679.pdf.

[90] FED. TRADE COMM'N, BUREAU OF CONSUMER PROT., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE–A REPORT TO CONGRESS iii, 4, (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[91] *Id.*

[92] *Internet Policy Task Force*, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, http://www.ntia.doc.gov/category/internet-policy-task-force (last visited Dec. 30, 2012).

agencies do not exclusively regulate data protection, and are not set up exclusively for the purpose of regulating the Internet. Presently, the NTIA serves as the President's principal advisor on communications and data policy.[93] The NTIA is responsible for working with other governments and international organizations to form compatible Internet policies, but it also works with businesses and other U.S. governmental agencies in order to develop new policies.[94]

Unlike NTIA, the ITA's scope is narrower and the portion of Internet policy that it focuses on is related to the U.S.-EU Safe Harbor Agreement.[95] The U.S.-EU Safe Harbor Agreement was formed in 2000 in order to facilitate the transfer of personal data between the U.S. and the EU.[96] Before the Safe Harbor Agreement, the EU states could not transfer data to the U.S. because the U.S.'s data protection policy was inadequate according to the standards of the European Commission.[97] The Safe Harbor Agreement created a set of guidelines for data protection that allowed for transmission of data between the U.S. and EU.[98] The ITA is responsible for managing the U.S.-EU Safe Harbor Agreement and must make sure the U.S.'s data policy conforms to the agreement.[99]

On the other hand, NIST is in charge of federal data protection on the Internet.[100] NIST, along with the Department of Defense and the Intelligence Community, produces Joint Task Force

---

[93] Lawrence E. Strickling, Assistant Secretary, NTIA, Speech at Hearing on Internet Privacy: The Views of the FTC, FCC, and NTIA (July 14, 2011), *available at* http://www.ntia.doc.gov/speechtestimony/2011/testimony-assistant-secretary-strickling-internet-privacy-views-ftc-fcc-and-nti [hereinafter Speech of Strickling].

[94] *Internet Policy*, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, http://www.ntia.doc.gov/category/internet-policy (last visited Dec. 30, 2012).

[95] *Id.*

[96] *U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, EXPORT.GOV, http://export.gov/safeharbor/ (last updated Mar. 22, 2011).

[97] *Id.*

[98] *Id.*

[99] Speech of Strickling, *supra* note 93.

[100] National Institute of Standards and Technology, *NIST Proposes New Privacy Controls for Federal Information Systems and Organizations*, NIST TECH BEAT (July 19, 2011), http://www.nist.gov/itl/csd/privacy-071911.cfm.

Transformation Initiative Documents.[101] NIST does not have a well-defined area of expertise in terms of data protection, and it appears that it overlaps a great deal with other agencies.[102] For instance, even though there is an Internet Policy Task Force, the NIST has its own Internet policy advisors.[103]

Lastly, the Internet Policy Task Force ("Task Force") is a newly formed agency whose purpose is to identify public policy and operational challenges in the Internet environment.[104] In 2010, the Task Force released a paper proposing the creation of a data protection agency.[105] In the paper, the Task Force argued that a data protection agency would be helpful because it would act as an "authority to convene businesses and civil society to develop effective, consensus-based voluntary codes of conduct in a wide variety of commercial contexts."[106] This proposed office will be part of the Department of Commerce.[107] Although this proposal was met with enthusiasm by those lauding the EU model of regulation, it is clear that this proposed office is really nothing new.[108] The agency will be like the Task Force itself, and it will work to facilitate communication between the private sector and the government in order to build upon the existing sectoral model.

Although the sectoral model is meritorious because it affords businesses freer rein in conducting its affairs and does not require the government to "babysit," so to speak, the sectoral model is far from perfect. Among the criticisms of the sectoral model is the fact that it is unwieldy and usually results in ineffective and spotty

---

[101] *Id.*

[102] William Jackson, *NIST To Get New Lead Internet Policy Advisor*, GCN (Aug. 10, 2010), http://gcn.com/articles/2010/08/10/ari-schwartz-to-take-policy-role-at-nist.aspx.

[103] *Id.*

[104] *Internet Policy*, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, *supra* note 94.

[105] DEPARTMENT OF COMMERCE, *supra* note 19.

[106] *Id.* at 44.

[107] *Id.*

[108] Peter Swire, *Getting Online Privacy Policy Right*, CENTER FOR AMERICAN PROGRESS (Jan. 28, 2011), http://www.americanprogress.org//issues/2011/01/privacy_office.html.

enforcement.[109] Precisely because a central authority is not involved in oversight of businesses, guidelines set out by the FTC are not followed across the board and, in addition, enforcement is difficult to carry out without a centralized body.[110] As to the self-regulatory aspect of the sectoral model, it is clear that putting a business in charge of protecting the rights of its consumers leads to a conflict of interest.[111]

III. THE EU MODEL

In contrast to the U.S. model, the EU online data privacy policy gives less freedom to businesses in conducting its business in the online privacy front. In 1995, the European Union passed its Directive on Data Protection,[112] which among other things, provided standards that member nations were required to follow. For instance, member states were required to ensure that personal information is to be "processed fairly and lawfully"[113] and "kept in a form which permits identification of data subjects for no longer than is necessary."[114]

The Data Directive is incredibly protective of personal information and regulates how the information is used, when it is used, and how the notification of data collection should be given.[115] Many have argued that the EU's emphasis on informational privacy stems from World War II and Germany's horrific past. The extensive government records that allowed Germany to single out its

---

[109] Ryan Moshell, . . . *And Then There was One: The Outlook For a Self-Regulatory United States Amidst A Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 367 (2005).

[110] *Id.*

[111] *Id.*

[112] Council Directive 95/46, art. 25, 1995 O.J. (L 281) (EC).

[113] Council Directive 95/46, art. 6(a), 1995 O.J. (L 281) (EC).

[114] Council Directive 95/46, art. 6(e), 1995 O.J. (L 281) (EC).

[115] EU countries have a well-defined basis for online privacy rights. On the other hand, U.S. law does not directly or specifically protect individual privacy. The Constitution does not protect individual privacy rights. *See* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of Internet*, 34 SAN DIEGO L. REV. 1153, 1185 (1997) (detailing the Constitution's lack of privacy protection for personal information and tracing Supreme Court decisions that have upheld that the Constitution does not recognize privacy for personal information).

Jewish citizens have led to a European concern for data privacy.[116] Whatever the reason for Europe's strong focus on privacy, it is clear that the EU has a stronger policy than that of the U.S. and at the foundation of this policy is the Data Directive.

The EU model of data protection is described as a comprehensive model in which an entity is set up to ensure that businesses and individuals are adhering to privacy protection laws.[117] The Data Directive provides the broad framework of rules that member states must then implement and add to in any way they please. The Data Directive provides eight main principles: (1) purpose limitation, (2) data quality, (3) data security, (4) special protection for sensitive data, (5) transparency, (6) data transfers, (7) independent oversight, and (8) individual redress.[118] The principle of purpose limitation requires that the information should only be collected to the extent that it is necessary for a specific purpose and that it is not stored any longer than is needed.[119] Data quality requires that information be updated.[120] Data security requires that reasonable measures be taken to provide secure data transmissions.[121] Next, the special protection for sensitive data principle forbids government from collecting information regarding the "racial or ethnic origin, political opinions, religious or philosophical beliefs . . . [or] concerning health or sex life."[122] The transparency principle stands for the idea that the person on whom information is collected should be notified of the fact.[123] The Data Directive requires not only that individuals be informed when information is collected about them but also that the person be informed of the identity of the collector and the purpose for which it will be used.[124] Next, under the data transfers principle, transfers of personal information to third

---

[116] *See* Moshell, *supra* note 109, at 358. Indeed, a look at the Data Directive's prohibition on government's collection of information regarding an individual's racial or ethnic background certainly seems to back this point.

[117] *Id.* at 366.

[118] Cates, *supra* note 21, at 173, 185–86.

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] Data Directive, *supra* note 22, art. 8(1).

[123] *See* Cates, *supra* note 21, at 186.

[124] *Id.*

parties are prohibited if done without consent of the data subject.[125] Also, under the independent oversight principle, an oversight body that will audit data processing systems and investigate complaints must be set up.[126] Lastly, the individual redress principle requires that individuals be provided with the right to access their personal information and enforce legal rights against those who wrongfully use their personal information.[127] In addition to these eight principles, the Directive also requires that EU members only exchange data with non-EU countries only if the non-EU country has an "adequate" data protection policy.[128]

In order to enforce the principles of the Directive, in 2000 the EU created a supervisory authority to oversee the EU community in regards to data policy protection.[129] This supervisory authority is called the European Data-Protection Supervisor and works independently from the European Parliament and Commission, meaning that it does not take orders from either.[130] The Supervisor's more specific duties include investigation of complaints and providing information to the EU community in general.[131] The Supervisor may exert power in the instance where "data processing is carried out in the EU and the data controller is established there."[132] The Supervisor may also exert power when the data controller is not based in the EU but in a place "where its national law applies by

---

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] *See* Data Directive, *supra* note 22, art. 3. This rule has been quite problematic for those countries wishing to obtain EU membership as well as those countries wishing to trade with EU nations. *See also* Eric Shapiro, *All is Not Fair in the Privacy Trade: The Safe Harbor Agreement and the World Trade Organization*, 71 FORDHAM L. REV 2781 (2003) (explaining how prospective EU members must conform to the EU's data policy in order to become a member).

[129] Authority for the EU Data Protection Supervisor was created in Regulation 45/2001. Council Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals With Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, ch.1, art. 1(2), 2000 O.J. (L 8).

[130] *Id.* at art. 44(1), (2).

[131] *Id.* at art. 46.

[132] Christopher Kuner, *Beyond Safe Harbor: European Data Protection Law and Electronic Commerce*, 35 INT'L LAW. 79, 82 (2001).

virtue of public international law." [133] Lastly, the Supervisor may also exert power when the "data controller is established outside the EU but equipment is used in the EU for the purposes of processing data."[134]

Now that we've examined the legal basis for the EU privacy regime, it is also necessary to analyze the implementation of the Directive. EU member states are given the freedom to implement the Directive in the way that each chooses, and each state has a unique way of carrying out the EU law. It is especially interesting to see the varying levels of power that each state has given its government in order to regulate data privacy. The policy question of how much power should be given to government to protect privacy shows how each country has managed to balance the competing interests of fundamental rights and state power. In addition, this topic is also important because the question lies at the very core of the U.S. data protection model. The different approaches that EU states have chosen will help determine whether a policy similar to the EU policy will be feasible in the U.S.

Two EU countries that best illustrate diverging approaches in the level of power it accords to government in regulating privacy are the U.K. and France. The U.K. has generally been careful about burdening companies and stepping too much on the toes of businesses in the process of protecting privacy. In addition, it has not enacted any overreaching laws that have interfered with existing rights. On the other hand, France has come under fire more than once for what some perceive as over-inclusive laws that infringe upon the liberties of its people.

A. The United Kingdom

In the U.K., the government body overseeing online privacy enforcement is called the Informational Commissioner's Office (ICO). The ICO was formed with the goals of transparency of businesses and information collectors and privacy of personal information. The ICO is a relatively young organization that has

---

[133] *Id.*
[134] *Id.*

developed a great deal since its humble start.[135] In its early days, the ICO consisted of only 80 people working in a single office.[136] Today, it has 4 offices with a total staff count of 353 and receives a little over 30,500 complaints a year.[137] Its goals are to promote transparency and data privacy for personal information.[138]

The ICO was created in 1984 and was originally titled the Data Protection Registrar until 2000 when it was given its current name.[139] It is tasked with enforcing the Data Protection Act of 1998, the Data Protection Telecommunications Directive (97/66/EC), the Privacy and Electronic Communications Regulations 2003, and the Environmental Communications Regulations 2003, and the Freedom of Information Act.[140] In addition, this body is also responsible for ensuring that the U.K. complies with EU rules.[141] Further, the ICO has a public record of all data controllers and requires all data controllers to register.[142] Although it is a government body, the ICO is given much relative freedom in that it is an independent regulatory agency that reports to Parliament.[143]

In order to enforce the data privacy policies for which it is responsible, the ICO has a number of means available to it. However the options it can exercise depend on whether the issue at hand concerns data privacy or transparency. In order to promote data privacy, the ICO has eight options on which it may proceed: (1) serve

---

[135] A large part of this growth should be credited to the Internet boom.

[136] Information Commissioner's Office, *History of the ICO*, ICO, http://www.ico.gov.uk/about_us/our_organisation/history.aspx (last visited Dec. 30, 2012). It is interesting to note that in its second year, the ICO only received eleven complaints throughout that year. *Id.* However, it is important to keep in mind that this was before the Internet became widely accessible.

[137] Information Commissioner's Office, *Key Facts*, ICO, http://www.ico.gov.uk/about_us/our_organisation/key_facts.aspx (last visited Dec. 30, 2012).

[138] *Id.*

[139] *Id.*

[140] Information Commissioner's Office, *Introduction to the ICO*, ICO, *available at* http://www.ico.gov.uk/about_us/our_organisation /introduction.aspx (last visited Dec. 30, 2012).

[141] *Id.*

[142] *Id.*

[143] Information Commissioner's Office, *History of the ICO*, *supra* note 136.

notices, (2) issue undertakings, (3) serve enforcement notices, (4) conduct assessments, (5) serve assessment notices, (6) issue fine notices, (7) prosecute wrongdoer, and (8) report to Parliament on pervasive issues.[144] When the ICO chooses to serve notices, it will give notice that an organization must turn over particular information to the ICO within a specified period of time.[145] When the ICO issues undertakings, on the other hand, it will require that an organization take a specific course of action in order to adhere faithfully to the rules.[146] Next, enforcement notices are commonly used when there has been noncompliance and these notices require that an organization take steps in order to comply with the law.[147] Then, there are assessments or audits in order to ensure compliance.[148] The serving of assessment notices is used to assess whether an organization is collecting personal data accordingly; this option is used for data protection only.[149] Next, fines of up to £500,000 may be issued for "serious" breaches of the Data Protection Act or the Privacy and Electronic Communications Regulations.[150] Then, of course, there is always the option to prosecute those who engage in

---

[144] Information Commissioner's Office, *Taking Action: Data Protection and Privacy and Electronic Communications*, ICO, http://www.ico.gov.uk/what_we_cover/taking_action/dp_pecr.aspx (last visited Dec. 30, 2012).

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] *See* Information Commissioner's Office, *Taking Action: Data Protection and Privacy and Electronic Communications*, *supra* note 144.

[150] *Id.* The ICO wasn't given the power to fine organizations until 2008. *See* Stuart Sumner, *Analysis: Should the ICO Wield the Carrot or the Stick?*, COMPUTING.CO.UK (Aug. 4, 2001), *http://www.computing.co.uk/ctg/analysis/2099482/analysis-ico-wield-carrot-stick*. Interestingly, Commissioner Graham has asked for the power to issue custodial sentencing for breaches under the Data Protection Act. *Id.*

The ICO's largest fine to date (£130,000) has been issued to Powys County Council for sending information about a child protection case to the wrong recipients. *See* Dan Raywood, *Largest ICO Fine Issued To Powys County Council for Two Breaches of Sensitive Data*, SC MAGAZINE UK (Dec. 6, 2011), http://www.scmagazineuk.com/largest-ico-fine-issued-to-powys-county-council-for-two-breaches-of-sensitive-data/article/218221/.

criminal acts under the Data Protection Act.[151] Prosecutions usually involve fines and a conditional discharge,[152] which means that the wrongdoer will not receive a punishment if they comply with certain rules for a period of time. Lastly, the ICO may report to Parliament in order to address data privacy issues.[153]

The methods that the ICO may use to promote transparency are not unlike those available to counter act data privacy issues, but there are some still minor differences. Just as with data privacy issues, the ICO may still tackle transparency issues by conducting assessments, serving information notices, issuing undertakings, prosecuting wrongdoers, and reporting to Parliament.[154] However, unlike with a data privacy issues, the ICO may issue practice recommendations and decision notices.[155] Practice recommendations are used to map out steps a public organization should take to uphold the codes. In the same vein, decision notices report the results of the ICO's investigation to "publically highlight particular issues with an authority's handling of a specific request."[156]

---

[151] Information Commissioner's Office, *Taking Action: Data Protection and Privacy and Electronic Communications*, *supra* note 144.

[152] *Id.* In addition to fines and conditional discharge, the ICO is also calling for "more effective deterrent sentences, including the threat of prison, to be available to the courts to stop the unlawful use of personal information." *See* Information Commissioner's Office, *Receptionist Unlawfully Accessed Sister-in-Law's Medical Details*, ICO (Dec. 16, 2011), http://www.ico.gov.uk/news/latest_news/2011/receptionist-unlawfully-accessed-sister-in-law-medical-details-16122011.aspx.

[153] Information Commissioner's Office, *Taking Action: Data Protection and Privacy and Electronic Communications*, *supra* note 144.

[154] *See id.*; Information Commissioner's Office, *Taking Action: Freedom of Information, Environmental Information and Spatial or Geographic Information*, http://www.ico.gov.uk/what_we_cover/taking_action/foi_eir.aspx (last visited Oct. 25, 2012).

[155] Information Commissioner's Office, *Taking Action: Freedom of Information, Environmental Information and Spatial or Geographic Information,* http://www.ico.gov.uk/what_we_cover/taking_action/foi_eir.aspx (last visited Oct. 25, 2012). In addition, the ICO may not issue assessment notices, which can only be used for privacy issues. But it seems that this would not make much of a difference because an enforcement notice essentially serves the same purpose as an assessment notice. *Id.*

[156] *Id*.

Despite the various means through which for the ICO can enforce the Data Protection Act, some still perceive it as toothless and inept.[157] This perception of ineptness has recently been furthered by the Leveson Inquiry.[158] During the Leveson Inquiry, Francis Aldhouse, a former head of the ICO, stated that media groups were "too big" for the ICO to confront despite the fact that the public body had clear evidence showing that journalists were engaging in phone hacking to obtain stories.[159] Although it is conceded that the ICO was not the only group afraid to step up to the powerful media conglomerates, the Leveson Inquiry was a blow to the ICO's reputation nonetheless.[160] Testimony about the ICO during the Leveson Inquiry and its subsequent criticism offers a telling portrait of how citizens feel about the organization. The Leveson Inquiry tackles a universally condemned breach of privacy, and it is

---

[157] *See* The Frontline, *ICO'S Reputation Takes a Hit After Leveson Testimony by Former Deputy*, V3.CO.UK (Dec. 1, 2011), http://www.v3.co.uk/v3-uk/the-frontline-blog/2129362/icos-reputation-takes-hit-leveson-testimony-deputy ("The [ICO] has never had an easy existence, many criticising it as a toothless watchdog before it had the power to fine organisations, and then complaining that it has failed to use this power correctly since it was introduced.").

[158] The Leveson Inquiry is an investigation into journalism practices sparked by the *News of the World* phone hacking debacle. *See Background, The Leveson Inquiry*, THE LEVESON INQUIRY, *available at* http://www.levesoninquiry.org.uk/ (last visited Oct. 11, 2012).

[159] *Leveson Inquiry: Watchdog Chief Francis Aldhouse 'refused to go after papers' Despite Steve Whittamore Hacking Evidence*, THE TELEGRAPH (Dec. 1, 2011, 7:21 AM), *available at* http://www.telegraph.co.uk/news/uknews/leveson-inquiry/8927424/Leveson-Inquiry-watchdog-chief-Francis-Aldhouse-refused-to-go-after-papers-despite-Steve-Whittamore-hacking-evidence.html.

[160] *See* The Frontline, *ICO'S Reputation Takes a Hit After Leveson Testimony by Former Deputy*, *supra* note 157 ("However, while it's easy to find fault with the ICO, the organisation was clearly one of countless groups, businesses and individuals that dared not incur the wrath of the Murdoch media empire, even if they were operating on behalf of the government.").

Testimony during the Leveson Inquiry revealed that many others knew about journalists hacking into phones. *See* Nick Davies, *Murdoch Papers Paid £1m to Gag Phone-Hacking Victims*, THE GUARDIAN (July 8, 2009, 5:33 PM), *available at* http://www.guardian.co.uk/media/2009/jul/08/murdoch-papers-phone-hacking. Despite this fact, however, the ICO's inaction in the face of glaring evidence appears especially egregious because the ICO is supposed to be an independent watchdog for UK citizens and, unlike other groups, had less of an interest at stake in confronting this unethical journalistic practice.

understandable that many would be angry at the ICO's inaction because of the emotionally polarizing subject matter. However, the overall sense of dissatisfaction towards the ICO reflects the consensus of many citizens that the group is incompetent.[161] The ICO's own monitoring reports evidence slow progress in bringing organizations and businesses up to speed with the Data Protection Act.[162] Even though a survey in late 2011 showed an improvement from past years, citizens are still dissatisfied with the ICO.[163] The recent survey showed that nearly three-quarters of firms were aware that they needed to protect personal information, which was a 26% improvement from the previous year's survey.[164] However, it is unclear whether firms are actually complying with the Data Protection Act.[165] In addition, three-fourths of citizens surveyed felt that online businesses were not adequately protecting their data.[166]

What's more, many U.K. citizens are unaware of the existence of the ICO.[167] According to a survey of 2,000 people conducted by OnePoll for the security company, LogRhythm, sixty-four percent of those polled did not know about the ICO, and of those that were aware of the ICO, only thirty-three percent believed that the

---

[161] *See* Stuart Sumner, *Analysis: Should the ICO Wield the Carrot or the Stick?*, COMPUTING.CO.UK (Aug. 4, 2001), http://www.computing.co.uk/ctg/analysis/2099482/analysis-ico-wield-carrot-stick.

[162] *See* Information Commissioner's Office, FREEDOM OF INFORMATION ACT PUBLICATION SCHEMES POLICE SECTOR MONITORING REPORT (March 2010), *available at* http://www.ico.gov.uk/what_we_cover/~/media/documents/library/Freedom_of_Information/Research_and_reports/POLICE_SECTOR_PS_MONITORING_REPORT.ashx (last visited Dec. 30, 2012); *See also* Simon Quicke, *ICO Reveals Patchy Progress From Firms Over Data Protection*, MICROSCOPE.CO.UK (Oct. 21, 2011), http://www.microscope.co.uk/news/reseller-news/ico-reveals-patchy-progress-from-firms-over-data-protection/.

[163] *See* Quicke, *supra* note 162.

[164] *Id.*

[165] *Id.*

[166] *Id.* This distrust is, in large part, a reaction to various news reports of businesses losing client information and police using information to snoop into citizens' personal lives. *Id.*

[167] LogRhythm, *Research Shows UK Public Losing Patience with Organisations that Endanger Customer Data*, LOGRHYTHM.COM (Oct. 19, 2011), http://logrhythm.com/company/press-releases/research-shows-uk-public-losing-patience.aspx.

group was adequately fulfilling its duties.[168] Perhaps the dissatisfaction stems from how the ICO enforces the law. The ICO has only recently been given the power to fine organizations and this power has worked to put some teeth into the once toothless data privacy group.[169] But now that the ICO has a stick with which to enforce the law, the question becomes whether or not the ICO should work directly with companies and organizations in order to guide them towards a data protection plan or whether fines should be issued.[170] For some organizations that already have their budgets spread thin a fine would be devastating.[171] However, the other side of the coin reveals that such organizations will be unlikely to risk another fine or a fine at all, and the threat of a fine would encourage businesses and organizations to be more careful about complying with the rules.[172] Lastly, the ICO is criticized for primarily targeting breaches made by the public sector.[173]

B. France

In France, the data protection authority is known as the Commission on Information Technology and Liberties (CNIL).[174] The word "information" in CNIL is incredibly broad and is defined to cover the "organization, processing, and transmission of personal information, normally by computers, but it also includes a concern for the implications of information systems for society."[175] CNIL was created by the January 6, 1978 Act and was intended to protect

---

[168] *Id.* LogRhythm is a company that provides products used for cyber security. *See About LogRhythm*, LOGRHYTHM.COM, http://www.logrhythm.com/Company/Overview.aspx (last visited Oct. 23, 2012).

[169] *See* Sumner, *supra* note 161.

[170] *Id.* Some believe that "[t]raining and education is the best way to prevent data breaches . . . ." *Id.*

[171] *See id.*

[172] *See id.*

[173] Peter Judge, *ICO Slaps Oldham School, But Suffers Fresh Criticism*, TECHWEEK EUROPE (Apr. 21, 2011), http://www.techweekeurope.co.uk/news/ico-slaps-oldham-school-but-suffers-fresh-criticism-27241.

[174] *See Its Status*, CNIL, http://www.cnil.fr/english/the-cnil/status/ (last visited Oct. 24, 2012).

[175] DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 176 (1989).

the privacy and individual rights of French citizens in the face of technological changes.[176] Like the U.K.'s ICO, CNIL is an independent agency.[177] Unlike the ICO, however, CNIL is more seamlessly integrated into its country's government.[178] While the ICO consists of members independent of Parliament, CNIL consists of several members who hold actual positions within the branches of government.[179] For instance, among the members of CNIL are four members of Parliament, two members of the Economic and Social Council, and six Supreme Court judges.[180] The five other members of CNIL do not hold seats in government.[181] Most recently, the French Data Protection Act was amended by a new law.[182] The new law provides for a new position within CNIL's plenary committee known as Defender of Rights.[183]

Four departments assist CNIL commissioners with their tasks: (1) Legal & International Affairs and Expert Appraisals; (2) Users Relations and Inspections; (3) Design, Innovation, & Expertise; and (4) Human Resources, Finance, IT, & Logistics.[184] CNIL's tasks consist of reviewing bills submitted to it by the government, issuing sanctions or warnings to noncompliant companies, conducting

---

[176] Commission Nationale de l'Informatique et des Libertés, *Its Status*, CNIL.FR, *available at* http://www.cnil.fr/english/the-cnil/status/ (last visited Oct. 25, 2012). The catalyst to the creation of CNIL was the government's SAFARI project which involved assigning numbers to each citizen in order to streamline records. *Id.* The public heavily criticized SAFARI, and feared total invasion of personal privacy. *Id.* So CNIL was formed to counteract these fears. *Id.*

[177] *Id.*

[178] This arm's length relationship with the government further complicates CNIL's independence, or lack thereof. FLAHERTY, *supra* note 175, at 185.

[179] *Id.*

[180] *Id.*

[181] *Id.*

[182] *See* Hunton & Williams, LLP, *French Data Protection Act Amended*, PRIVACY AND INFORMATION SECURITY LAW BLOG (Mar. 31, 2011), http://www.huntonprivacyblog.com/2011/03/articles/french-data-protection-act-amended/.

[183] *Id.*

[184] Commission Nationale de l'Informatique et des Libertés, *Its Operation*, CNIL.FR, *available at* http://www.cnil.fr/english/the-cnil/its-operation/ (last visited Oct. 24, 2012).

investigations, and informing the public of its rights and obligations.[185]

CNIL has the power to regulate, inspect, sanction, and keep inventory of existing processing operations.[186] Under CNIL's regulatory power, companies or entities wishing to implement a public file must first receive an affirmative ruling from the body.[187] Under its investigatory power, CNIL has the right to investigate complaints and to monitor the security of data processing.[188] In addition, according to the August 6, 2004 Act, CNIL may either impose sanctions of up to €300,000 or it may issue warnings, depending on the type of breach.[189]

CNIL has been criticized for its lack of independence from the government. Critics have claimed that CNIL has leaned towards supporting the government rather than remaining faithful to its original purpose of protecting data privacy and citizens' rights.[190] As mentioned earlier, CNIL was created in response to criticism of the government program SAFARI, which was a project creating a database documenting each citizen.[191] It appears that CNIL was originally created to protect French citizens from government intrusions to privacy. In this respect, citizens regard CNIL as abandoning its duties.[192]

Recently, the French government passed a law named LOPPSI 2 that allows blocking Internet access without a court order to sites containing child pornography.[193] Although those opposed to

---

[185] *Id.*

[186] *Missions and Powers*, CNIL, http://www.cnil.fr/english/the-cnil/operation/ (last visited Oct. 24, 2012).

[187] *Id.*

[188] *Id.*

[189] Commission Nationale de l'Informatique et des Libertés, *supra* note 184.

[190] Chloe Leprince, *Cnil: trente ans contre la << tyrannie de l'ordinateur >>* [*CNIL: Thirty Years Against the "'Tyranny of the Computer'"*], RUE 89 (Jan. 6, 2008), http://www.rue89.com/2008/01/06/cnil-trente-ans-contre-la-tyrannie-de-lordinateur.

[191] *See supra* note 176.

[192] *See supra* notes 161–166 and accompanying text.

[193] *France: Loppsi 2 Adopted-Internet Filtering Without Court Order*, EDRI (Feb. 23, 2011), http://www.edri.org/edrigram/number9.4/web-blocking-adopted-france-loppsi-2.

the law challenged it in the Constitutional Council, the law was declared to be valid under the French Constitution.[194] This law was heavily criticized by French citizens who saw it as censorship of the Internet.[195] Although the CNIL voiced its reservations in preliminary drafts of LOPPSI 2, French citizens felt that this was not enough.[196] Indeed, it was even more shocking to French citizens that the president of CNIL, Alex Tüurk, ended up voting for LOPPSI 2.[197] Despite these critiques, CNIL does appear to be dogged in its protection of privacy. In 2011 it fined Google €100,000 for collecting passwords, email messages, and login names while taking pictures for Street View.[198]

IV. COMPARISON OF THE EU AND U.S. MODELS

In comparing the U.S. and EU models, one can see many differences and some similarities at both the legislative and enforcement levels. At the legislative level, the EU regime appears more streamlined and less complex than its U.S. counterpart. For example, the EU relies on only one law to provide the right to informational privacy for citizens of EU states. In contrast, instead of relying on one law to grant privacy protection, the U.S. relies on a multitude of laws, such as the GLBA and HIPAA, to secure privacy. Because the U.S. model relies on narrowly tailored laws to carve out privacy rights, data protection in the U.S. depends upon various factors, such as the type of information in question and the type of business in question. Thus, U.S. citizens are is not given the right to privacy of any and all personal information; rather, the right to

---

[194] *Loppsi 2 Bill Passes the French Constitutional Council Test*, EDRI (Mar. 23, 2011), http://www.edri.org/edrigram/number9.6/loppsi-2-adopted.

[195] *See* Leprince, *supra* note 190.

[196] Christophe Auffray, *Loppsi 2: la CNIL émet toujours des réserves* [*Loppsi 2: the CNIL Still has its Reservations]*, ZDNET.FR (June. 23, 2011), http://www.zdnet.fr/actualites/loppsi-2-la-cnil-emet-toujours-des-reserves-39752653.htm.

[197] Juliean L., *Le président de la CNIL justifie son vote des Loppsi et Hadopi* [*The President of the CNIL Justifies His Vote and Loppsi and Hadopi]*, NUMERAMA (Feb. 8, 2011), http://www.numerama.com/magazine/17999-le-president-de-la-cnil-justifie-son-vote-des-loppsi-et-hadopi.html.

[198] *France Fines Google Over Street View Data Blunder*, BBC NEWS (Mar. 21, 2011), http://www.bbc.co.uk/news/technology-12809076.

privacy depends on the type of information and whether or not the sector of industry controlling the data is subject to regulation. On the other hand, EU informational privacy is not bound by such factors because the Directive grants a broad right to privacy across the board, regardless of the type of business or information involved.

Interestingly enough, however, when the eight principles of the Directive are compared to the multiple U.S. laws, we can see that a number of U.S. laws strive to accomplish the same goals as the Directive. It must be noted, however, that because of the way it is set up, the goals of the U.S. system really depends on the laws in place and each law varies one from the next. Recall that the eight goals of the EU law are: (1) purpose limitation, (2) data quality, (3) data security, (4) special protection, (5) transparency, (6) data transfers, (7) independent oversight, and (8) individual redress.[199] The Directive goals that many U.S. laws target are: data quality, data security, transparency, data transfers, and individual redress. The fact that the U.S. framework allows users to update or correct information to achieve the end-goal of data quality is not surprising because it is in the best interests of businesses to do so—just look at your Google or Amazon account, it will most likely allow you to change or add to your address and credit card information. However, there are laws that also strive to protect the best interests of citizens, including HIPAA and FCRA.

Next, the U.S. model also shares the goal of data security in that it requires businesses to take reasonable measures to provide data security. In addition, the U.S. model also encourages transparency by requiring companies to give notice. The most notable laws providing for notice are GLBA, HIPAA, FCRA, COPPA, and, on the state level, California's security reporting statute, California Civil Code § 1798.82. Unlike the business-driven aim of data quality, the goal of transparency seems to be driven by legislatures more than industry practice.

Next, the U.S. model also shares with the Directive the goal of protecting data transfers. This goal, however, is closely intertwined with the aim for transparency, and the U.S. uses the same transparency mechanisms of notice and opt-out to protect data transfers. Lastly, the U.S. also provides its citizens with the option

---

[199] *See supra* discussion at 830–31.

for individual redress. An individual may sue businesses under some federal statutes and state laws if her personal information is mishandled. In the end, the EU Directive and U.S. models do share a great deal of similarities on the theoretical level.

In application, however, the differences that do exist between the two models inevitably lead to differences on the enforcement level also. The EU model's reliance on solely the Directive to grant privacy protection and the broad rights that the Directive provides, results in a fairly straightforward and predictable application. In contrast, the fact that the U.S. model rests on various laws, which are further derived from different sources—contracts, tort, state, and federal—adds to the complexity of its policy. This complexity in the U.S. policy yields unpredictability and confusion for both industry and citizens. For instance, different laws create different legal standards. Under contract principles, a company may be required to provide notice, choice, and access to any transfer of personal information. Under tort law, if negligence is invoked, a company would need to be held to the same duty of care as that practiced by others in the same industry. In addition, there may be standards imposed by federal and state law. The various possible standards make it difficult for a company to determine its level of responsibility. In the same vein, it also creates unpredictability for a potential plaintiff seeking redress. Some have noted that class action suits relying on contract claims have been more successful than those relying on federal statutes, which are usually inapplicable.[200]

Comparison of the EU and U.S. models reveals some similarities but also vast differences. One difference that makes the U.S. model weaker in comparison to the EU model is the patchwork of laws the former employs. These laws create a complex and often confusing system that frustrates both businesses and private citizens alike. On the other hand, the EU model has only one source that provides the right to data protection, which makes for a more straightforward, simple system. Despite these differences, however, the U.S. and the EU do share similar policy goals. So, it is not the U.S. laws themselves that need reworking because it is the

---

[200] *See* Sobel et al., *supra* note 33, at 61 (noting that federal statutes sometimes did not provide for the more common types of data misuse).

application of the laws that create the differences between the EU and U.S. models.

V. AN EXACT DUPLICATION OF THE EU MODEL WILL NOT WORK IN THE U.S.

There is undoubtedly a need for a stronger data protection regime in the U.S., but an exact duplication of the EU model is not the answer. If the U.S. were to adopt the EU model, it would first have to pass something identical to the Directive because the Directive is the legal foundation for the EU's data protection policy and the very heart of the EU model. As mentioned before, the Directive essentially guarantees citizens a right to informational privacy. One glaring problem that the U.S. would have if it were to pass a Directive-like law would be the validity of the law. Even though the right to privacy has been recognized in the U.S., case law shows that this right is not limitless and is subject to a number of qualifications.

Although the Constitution does not explicitly provide a right to privacy, the Supreme Court has read this right into the document. The most notable Supreme Court cases establishing this right are *Griswold v. Connecticut* and *Roe v. Wade*. In *Griswold*, the Court had to decide on the constitutionality of several Connecticut statutes that forbade the use of contraceptives by married couples.[201] Expanding upon its previous rulings upholding personal autonomy, the Court held that the Constitution also guaranteed generally, the right to keep private matters from disclosure and, specifically, the right of marital privacy.[202] Despite the fact that the Constitution

---

[201] Griswold v. Connecticut, 381 U.S. 479, 480 (1965).

[202] *Id.* at 486. The Court had previously upheld personal autonomy in a variety of cases. *See* Skinner v. Oklahoma, 316 U.S. 535, 541 (1942) (striking down a statute that allowed for sterilization of criminals, stating that procreation is "one of the basic civil rights of man"); Pierce v. Soc'y of Sisters, 268 U.S. 510, 534–35 (1925) (Court struck down an Oregon statute requiring children to attend public schools, stating "the [statute] unreasonably interferes with the liberty of parents . . . to direct the upbringing and education of children under their control."); Meyer v. Nebraska, 262 U.S. 390, 399–401 (1923) (Court struck down a Nebraska law prohibiting foreign languages from being taught to schoolchildren under the reasoning that parents had a right to determine what their children should learn, and teachers had a right to teach the subjects of their choosing.).

itself does not mention privacy, it was a legitimate right nonetheless because "[v]arious [constitutional] guarantees create zones of privacy."[203] *Griswold* is important not only because it cemented the right of privacy, but also because it defined privacy. Here, privacy was defined as the right of protecting private matters from disclosure and intrusion by the State.[204]

Eight years after *Griswold*, the Court decided the case of *Roe v. Wade* and expanded its definition of privacy to include personal autonomy.[205] This controversial case dealt with a set of Texas statutes that criminalized abortion.[206] Citing to a string of cases that had upheld the right to privacy, the Court concluded that such a right included a woman's decision to terminate her pregnancy.[207] However, the Court noted that this privacy right of personal autonomy "cannot be said to be absolute" and that there are situations in which a state may properly intervene in areas protected by the right.[208]

From *Griswold* and *Roe v. Wade*, we get two definitions of privacy—personal autonomy and freedom from intrusion and disclosure. It is interesting to note that these seminal privacy cases involved governmental and not a private third-party intrusion on privacy. So whether or not privacy rights can be enforced against private third parties is a question that the Court has left unanswered. In addition, informational privacy is not like any other privacy right that the Court has come across, and it is unclear whether the Court would be willing to expand its definition of "privacy" to include informational privacy. In *Whalen v. Roe*, for instance, the Court allowed the state of New York to maintain a database containing names of those who have acquired prescription drugs known to be sold on the illegal market.[209] The Court stated that it was possible that the Constitution provided for informational privacy, but it

---

[203] *Griswold*, 381 U.S. at 484.

[204] JONATHAN D. VARAT ET AL., CONSTITUTIONAL LAW 632 (13th ed., 2009).

[205] Roe v. Wade, 410 U.S. 113 (1973).

[206] *Id.* at 117–18.

[207] *Id.* at 152–53.

[208] *Id.* at 154.

[209] Whalen v. Roe, 429 U.S. 589 (1977).

declined to decide on the matter.[210] As such, the Court appears wary of addressing this issue, and when the opportunity to decide on the matter came up once more in the case of *NASA v. Nelson*, the Court dodged the issue.[211]

Even assuming that the Court will incorporate informational privacy into the current privacy right, the constitutional issue will still be further complicated because the protections to privacy that citizens have against the government are weak. If the privacy protection is not ironclad even as against the government, and this right is constitutionally protected, we can assume that the protection of privacy that citizens have against private parties (something that is not constitutionally protected) will be even weaker. Indeed, the U.S. legal framework carefully protects the free flow of information, and a wholesale adoption of the restrictive EU model would act as a major roadblock to this important tenet of American jurisprudence. As discussed previously, the EU model affects the collection, use, and distribution of personal data.[212] At the very core of the American system of democracy is freedom of information. It is something that we take pride in because we feel that it sets us apart from countries that oppress and censor their citizens. The EU model gives citizens a lot of control over their personal information. Thus, if the U.S. adopts this model, it would conflict with decades of case law allowing for dissemination of information and free flow of information.[213]

Moreover, an exact replica of the EU model for the U.S. will not work because the U.S. already has a model in place, and that model is completely opposite to that of the EU model.[214] It would follow then, that if the U.S. adopted the EU model, the adoption

---

[210] *Id.*

[211] NASA v. Nelson, No. 09-530 (2011), *available at* http://www.supremecourt.gov/opinions/10pdf/09-530.pdf.

[212] Assey & Eleftheriou, *supra* note 20, at 148.

[213] *See* TIME, Inc., v. Hill, 385 U.S. 374 (1967) (holding that the *Times* standard privilege precluded recovery under a New York statute that allowed for recovery when a publication contained factual inaccuracies in matters of public interest); New York Times v. Sullivan, 376 U.S. 254 (1964); Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1229, 1234–35 (7th Cir. 1993) (Seventh Circuit ruled that a book depicting details of the Haynes's relationship, including the husband's alcoholism, did not invade their privacy).

[214] *See* discussion, *supra* 815.

would have the effect of razing the current system in favor of a completely different system. Practically speaking, it would be impossible to uproot the system and start anew from the ground up.

VI. TAKING THE MIDDLE ROAD

Even though a wholesale adoption of the EU model would not work in the U.S., that doesn't mean that the U.S. shouldn't borrow from the EU model. The U.S. doesn't have to pass sweeping laws or take extreme measures in order to improve its data protection model; rather, it can implement smaller measures. The goal should be to find a plan that works within the U.S. form of government—one that is compatible with its existing laws, political history, and culture. To this end, the U.S. would benefit from borrowing some ideas from the EU model, but should still keep the main framework on which the existing model is built.

At present, the U.S. has a data privacy model that works within its constitutional structure. This model combines a variety of federal and state laws based on tort and contract principles with a process-oriented approach.[215] Because these laws aren't grounded in constitutional rights, they provide a legitimate basis for data protection. In other words, these laws will not fall if they are attacked on constitutional grounds. However, this is not to say that the data policy is perfect. Although it is true that grounding the data protection laws on torts and contract principles works within the U.S. system, the laws are still disjointed. The current privacy protection policy we have does not adequately protect data from getting into the wrong hands.

A. Stronger Enforcement of Data Protection Laws

As recent developments in current events show, the U.S. system at present is not equipped to handle breaches of privacy, and

---

[215] *See* Smedinghoff, *supra* note 33, at 24 (noting that the FTC, states, and industry sectors are moving towards a trend that approaches data privacy using the "process oriented" legal standard in which an organization will "engage in an ongoing and repetitive process that assesses risk, identifies and implements responsive security measures, [and] verifies that they are effectively implemented.").

there is still more that should be done. For instance, some companies storing clients' credit card information don't encrypt their files, which is a very basic step that one takes to protect sensitive information. One could make the argument that the U.S. system places too much faith in the market, and allowing companies to self-regulate data protection naturally leads to the problem of conflict of interest. On one hand, businesses are delegated the duty of protecting customer information. On the other hand, businesses need to make a profit, and selling information is very lucrative.[216] Even if a company is not selling information, it lacks incentives to take that extra step to provide a sufficient level of data protection. The U.S. model, as it is now, is not practical and doesn't work. As Professor A. Michael Froomkin of the University of Miami Law School notes in his article "The Death of Privacy?," the "regulation" part of "self-regulation" is more-often-than-not overlooked.[217] He states that the existing plan is unworkable: "It may be that competitive pressures might ultimately drive firms to seek privacy certification, but currently fewer than 1000 firms participate in either TRUSTe's or BBBOnline's programs, which suggests that market pressure to participate is weak to nonexistent."[218] Businesses are responsible only to themselves, and without an outside force driving change, it is difficult to bring about any sort of data protection. Froomkin further adds that because the U.S. endorses self-regulation "without legal sanctions to incentivize it or enforce it; it is hard to believe that the strategy is anything more than a political device to avoid regulation."[219]

It seems then that the problem with the U.S. model is not that the data protection laws are flawed; rather, it is the enforcement of the laws that is lacking. It's not that there is an absence of federal laws or state laws protecting data protection, it is non-compliance to

---

[216] David Goldman, *Your Phone Company Is Selling Your Personal Data*, CNN MONEY (Nov. 1, 2011), http://money.cnn.com/2011/11/01/technology/verizon_att_sprint_tmobile_privacy/index.htm.

[217] A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1524–25 (2000) ("Without some sort of government intervention to encourage self-regulation,"[w]olves self-regulate for the good of themselves and the pack, not the deer.").

[218] *Id.* at 1527.

[219] *Id.*

these laws that is weakening the U.S. model.[220] This begs the politically charged question of: "Should the government play a stronger role in enforcing these laws?" This question should be answered in the affirmative. One of the most important things we should borrow from the EU model is the idea of government involvement in data regulation. Some government involvement is needed to provide the data protection that is vital in today's technology-laden society. This is not a call for total government control of data protection regulation, nor is it an argument that we must have the same level of government involvement as the one the EU model has. In other words, it is not suggested that the U.S. should enact laws or encourage laws that allow for filtering of the web, like LOPPSI 2. This paper only argues that government should play a stronger role than the one it has now. There should be enough federal regulation to encourage businesses to provide sufficient data security, but not so much regulation that businesses are unnecessarily burdened. Businesses should still maintain a role in data protection in the sense that the government should work with businesses and listen to feedback.

It could be argued that more government involvement would pose a burden to businesses and corporations. Admittedly, businesses should have the freedom to make their own decisions and act in any way that would best serve their shareholders. However, they still owe a duty to their consumers to take reasonable data security measures. More government enforcement would not mean that the government would step in to control the decisions companies make, it would only mean that companies would have to start complying with existing law. In addition, if the U.S. adopted stronger government enforcement without changing or adding any new privacy protection laws, the obligation placed on businesses would not be that much different than the obligation they now have.

Lastly, one could suggest that we could divide responsibility of rule enforcement between the government and the people. The people could help enforce the various laws in place through their right of redress. This wouldn't reflect the system that we have now because the U.S. is a highly litigious society with a legal system set up in a manner that encourages litigation. The right for a person to

---

[220] *See* 15 U.S.C. § 45(a).

have her "day in court" is important. Class action litigation can pose an effective measure for preventing lax data security by companies. Although this measure may be less costly than increased government involvement, it may not be very effective. At present, there are several statutes under which a private citizen may sue, including HIPAA and GLBA.[221] In addition, most of the actions that the FTC has brought against businesses for failing to provide adequate data protection have been based upon section 5 of the FTC Act, and these claims are deeply grounded in contract principles.[222] In fact, they are almost exclusively rooted in contract principles because a person doesn't own his or her personal information, and as of yet, there is not a strong constitutional right protecting privacy. While contract law is an effective means of regulating data security, the problem with rights under contracts is that such rights can be forfeited by agreement. One can easily imagine a situation where an individual must forego data security or a right to sue in order to receive a company's product or business. This happens quite often now with contracts requiring an individual to enter into arbitration, and foregoing his or her right to bring suit. If such a right can be contracted away, the whole idea of the right of redress falls on its face. Even though spreading the responsibility of enforcement between government and citizens may be a good alternative to increased government intervention, in the end, such an idea may fail to be effective because the right to sue can be contracted away.

B. Room for a U.S. Data Protection Agency

In borrowing from the EU model, the U.S. should not only increase government enforcement into its policy, it should also form a data protection agency. If this were to happen, it would help the U.S. model to effectively enforce data protection laws. One problem with the current model is that there are many different divisions, from the FTC to NTIA to the ITA to NIST, that handle data protection; this despite the fact that what is really needed is one coordinated and streamlined agency. Another problem with the current model is that

---

[221] Ian C. Ballon, *The Coming Wave of Internet-Related Security Litigation*, *in* SECURING PRIVACY IN THE INTERNET AGE 46 (Anupham Chander, et al., ed., 2008).

[222] *See* Sobel, et al., *supra* note 33, at 64.

the two main agencies that handle data protection issues at present, the FTC and the Department of Commerce, have other duties requiring agency focus, so they have to divide their time among their many responsibilities. Clearly, the FTC and Department of Commerce first started handling data protection issues because most laws that protect consumer information are aimed at business sectors. Thus, it would initially seem that the FTC and Department of Commerce are better equipped to handle issues of data protection. But we must also keep in mind that these two bodies handle a variety of different issues, and it is unlikely that these two agencies will be able to adapt quickly to changes in technology. In order to effectively enforce data protection, a lot of time, effort, and manpower will be needed. This may have the effect of spreading these two agencies thin. It will have the result of either detracting from their other duties, or they will not be able to effectively enforce data protection laws.

With laws at both the federal and state levels that target numerous sectors, an agency with a sole focus on data protection would be more adept at identifying and resolving problems. The red tape and inefficiency involved with having multiple data agencies effectively maims any enforcement measures that the government would take. Consolidating the data protection tasks into one unit would help the government act as a coordinated body.

So if a data protection agency were formed, what would it look like? An examination of the UK and French data protection agencies show that the agency must have teeth. The easiest way to give an agency power is to give it the ability to penalize breaches through fines. Without the power to fine, an agency will not have the power it needs to be effective. While this idea of fining data breaches would be a new practice in the U.S., it wouldn't be much different from the accepted U.S. practice of fining corporations for breaches of environmental law.[223] Thus, it wouldn't be such a radical idea as to be unacceptable to U.S. citizens. However, like the European data agencies, there should be a limit to the amount for

---

[223] Peter Henning, *Looking for Liability in B.P.'s Gulf Oil Spill*, NEW YORK TIMES DEALBOOK (June 7, 2010), http://dealbook.nytimes.com/2010/06/07/looking-for-liability-in-bps-gulf-oil-spill/ (describing fines for environmental breaches).

which a company can be fined if it fails to provide reasonable data protection. Fines should not be so low as to amount to a slap on the wrist, but the data protection agency also should not be given a carte blanche and hand out astronomical fines.

Finally, such an agency must be independent from government, because in the end, the agency's purpose is to look after citizens' rights. It must be on guard against infringements on such rights, whether the stifling of those rights comes from government or private parties. In France, CNIL is so intertwined with government that it seems to lose focus on its original purpose of protecting citizens' rights. It protects citizens from businesses, but many perceive the CNIL as inadequately protecting them from government.

C. Prevention First

Also, like the EU data protection agencies, the main focus of the U.S. data protection agency should be to prevent breaches. Currently, the FTC and the Department of Commerce only act to identify breaches that have already been made rather than identifying potential breaches. In contrast, the ICO as well as CNIL both assess company compliance to data protection laws and focus mainly on preventing data breaches by ensuring that the rules are being followed. So, in this way, the U.S. policy is more concerned with penalizing breaches rather than preventing them through assessments and performance reviews, contrary to the EU policy. Even without a data protection agency, the U.S. should still borrow this EU notion of prevention. Data security is becoming more of an issue with courts and agencies are applying various laws in new ways. For instance, the FTC's recent interpretation of FTC Act section 5 as applying to security breaches as an unfair trade practice[224] was a novel approach that was not communicated to companies. If companies had been put on notice, it is possible that there may have been changes that would have benefitted consumers and the companies that were in breach of this "unfair trade practice." In light of this, it would be helpful for companies to be warned before the law is applied in a novel way. If agencies were focused on prevention and performing assessments,

[224] *See* discussion, *supra* 823–24.

companies would have notice about what is expected of them and, hopefully, would be less susceptible to breaching data security laws.

VII. POSSIBLE CRITIQUES OF "MIDDLE ROAD" CONCEPT

Even though this "middle-road" idea may seem odd considering that the U.S. and EU models approach data protection from different ends of the spectrum, the idea will be workable. It is important to note that the two models are considered as radically different from each other only because the EU provides that privacy is a fundamental right while the U.S. does not. So, even though the EU policy may seem to conflict with U.S. policy, the U.S. will still be able to integrate some EU ideas into its current policy without creating contradictions.

If the U.S. were to adopt the EU's stance on government intervention, create a data protection agency, and focus on prevention of data breaches, the new changes would translate to the U.S. system. Some may argue that this would give too much control to the government, but one must keep in mind that some sacrifices have to be made in order to obtain benefits. It all boils down to the task of balancing the value of data protection against the value of moderate governmental intrusion. Thus far, the U.S. policy has tried to find a way in which it will not have to make any sacrifices—attempting to find a way in which it can have a hands-off government and adequate data protection. This desire to have the best of both worlds simply isn't feasible and proof that it isn't feasible lies in the state of U.S. data protection today. Self-regulation overly burdens companies because it expects a business to act as a neutral party to protect customer rights, even though businesses are anything but an indifferent party. Such an approach is not practical.

In balancing the right of data privacy protection against that of governmental intrusion, we must look at the level of governmental intrusion that is acceptable in the U.S. If the U.S. were to step in with a data protection agency and increase its regulation of data security, it wouldn't be any different from the FCC stepping in and regulating media[225] or the FTC regulating consumer rights.

---

[225] FCC v. Pacifica Found., 438 U.S. 726 (1978) (ruling that the FCC may restrict "indecent" broadcasting material).

Weighing this against protection of sensitive information, it would seem that data protection might outweigh the accepted practice of moderate government intrusion. Consumer information is highly sensitive and may create lasting problems if it gets into the wrong hands. In addition, modern technology allows information to be gathered quickly and in vast amounts. The gravity of harm that could be done to a multitude of people may outweigh the accepted practice of government regulation. Further, while heavier enforcement than the current level will not be overly welcome, it wouldn't be that great of a departure from our current system.[226] The FTC has been increasing its regulation of data protection, so an increase in enforcement will not vary greatly from the way the system runs now.

VIII. CONCLUSION

No system is perfect and the U.S. model of data protection is not an exception. However, one can be encouraged that the U.S. has a strong framework upon which to build. While we do not need to duplicate the EU model, there are several portions of the European model that we should borrow. With stronger enforcement and early detection of mistakes in data security, the U.S. will have a system that provides its citizens with the informational security that is needed in today's ever-changing world.

---

[226] Cheryl Morris, *Former FTC Director Talks Online Privacy – Facebook, Google & Startups*, BOSTONINNO (Apr. 7, 2011), http://bostinno.com/2011/04/07/former-ftc-director-talks-online-privacy-%E2%80%93-facebook-google-startups/.