DATA PROTECTION LAWS: QUILTS VERSUS BLANKETS

Samantha Diorio[†]

CONTENTS

INTRODUCTION 486
I. THE CONCEPT OF PRIVACY IN GENERAL & INTERNET COMPLICATIONS 489
II. BACKGROUND OF U.S. LAW 491
A. Patchwork System of Laws 491
1. Historical Background in American Law 491
2. FTC Regulation of Online Privacy 493
3. Sporadic State Regulation 495
III. DIVERGENT NOTIONS OF PRIVACY 497
A. Europeans and Personal Dignity 498
B. Americans and Liberty 499
C. Liberty and Dignity Diverge 500
IV. PRIVACY LAW'S EVOLUTION IN THE E.U. 501
A. Basic Principles of the E.U. Data-Protection Regime 501
B. Germany: The E.U.'s Strictest Data Collection Laws 502
C. United Kingdom: Least Stringent Data Collection Laws in the E.U. 503
V. COMPARING DATA COLLECTION PRIVACY LAWS IN THE UNITED STATES AND EUROPEAN UNION 504
A. Princess Caroline of Monaco 505
B. Sipple v. San Francisco Chronicle, Inc. 507
VI. WHETHER OR NOT THE E.U. SYSTEM WOULD WORK IN THE U.S. 508
A. Where Should the Law Go in the Future? 508
B. South Africa Implementing European-like Laws 509
CONCLUSION 511

---

† Samantha Diorio is a May 2015 graduate of Syracuse University College of Law.

INTRODUCTION

Send a card, some flowers and be prepared to pay your respects; the age of privacy is dead. At least this is how Facebook founder Mark Zuckerberg sees it. According to the chief executive of the world's most popular social networking site, Facebook, "[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."[1] To Zuckerberg, and an increasing number of others, the rise of social networking online means that people "no longer have an expectation of privacy" when they choose to utilize social media.[2] Zuckerberg's comments underscore not only the pervasiveness of social media and online technology, but also its implications on an individual's privacy in today's technological age. And it would seem that his observations are not without merit. With over one billion people using Facebook, it seems as though more and more people are using electronic media to post, upload, or share their most personal and private details, arguments, and disputes.[3] For many, yesterday's journal entry is today's Facebook post or Twitter tweet.

This was the exact mentality of 24-year-old law student Max Schrems from Salzburg, Austria.[4] With all the personal information that he knew he shared online, he decided that he wanted to know exactly what Facebook knew about him.[5] So he requested his own Facebook file.[6] What he received from Facebook both frightened and fascinated him; a virtual autobiography at 1,222 pages long.[7] The file had wall posts that had been deleted, old messages to friends that discussed a friend's difficult past, even information about his precise locations that

---

1. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010, 8:58 PM), *available at* http://www.theguardian.com/technology/2010/jan/11/facebook-privacy (last visited Apr. 22, 2015).

2. *Id.*

3. Cooper Smith, *7 Statistics About Facebook Users That Reveal Why It's Such A Powerful Marketing Platform*, BUS. INSIDER (Nov. 16, 2013, 8:00 AM), *available at* http://www.businessinsider.com/a-primer-on-facebook-demographics-2013-10 (last visited Apr. 22, 2015).

4. Somini Sengupta, *Should Personal Data Be Personal?*, N.Y. TIMES (Feb. 4, 2012), *available at* http://www.nytimes.com/2012/02/05/sunday-review/europe-moves-to-protect-online-privacy.html?pagewanted=all (last visited Apr. 22, 2015).

5. *Id.*

6. *Id.*

7. *Id.*

he did not enter himself.[8] When asked how he felt about such personal information being collected by Facebook, Schrems responded that he was mostly concerned about what Facebook could do to him in the future with all that information.[9] He wondered why all that information was kept when he clearly deleted it from his profile. "'It's like a camera hanging over your bed while you're having sex. It just doesn't feel good,' is how [Schrems] finally put it."[10] Mr. Schrems's reaction is illustrative of the distress sweeping across the globe about the ways in which Internet companies are treating and storing personal information.[11] It is this ever-present existence of technology that has Europeans and Americans alike confronting head-on the issue of how privacy law can function in an age of constant data collection.[12] It has become clear that with new technologies appearing quicker and quicker, privacy laws have become more difficult to keep up and craft to ensure adequacy.[13]

This note will explore whether the European Union's privacy laws could serve as a model for the United States. Currently, the United States' data protection laws can be seen as a patchwork system of laws coming from the state and federal levels, in addition to regulations imposed by various agencies.[14] In contrast, the European Union's 1995 Directive on Data Protection mandates that every member of the E.U. pass laws on the national level that will protect their citizens' privacy.[15] While the E.U. Model is vast and widespread, it also allows for some variation by permitting member states to craft their own laws.[16] This note will investigate how the United States should take a more comprehensive approach in regulating online privacy law and protecting its citizen's legal rights to protect their personal data.

The United States should implement baseline privacy protections that seek to cover a broad array of personal data, ensuring coverage of information that is not currently covered by fragmented privacy laws. In contrast to the U.S., the European Union has a far-reaching set of

8. *Id.*
9. Sengupta, *supra* note 4.
10. *Id.*
11. *Id.*
12. *See id.*
13. *See id.*
14. *See, e.g.*, The Online Privacy Protection Act (OPPA) of 2003, CAL. BUS. & PROF. CODE § 22575-22579 (Deering 2004); The Health Insurance Portability and Accountability Act of 1996 (HIPAA), 110 Stat. 1936 (1996).
15. Council Directive 95/46, art. 189b, 1995 O.J. (L 281) 31 (EC).
16. *Id.* para. 9.

legal rights that serve to protect personal data online. Every country in the E.U. has a statute that establishes proper practices in collection, storage, use, and disclosure of personal information. However, "[t]he E.U. model also allows for variation" in how a particular member state collects data, "by allowing its member countries to determine their own laws."[17] This slight flexibility may serve as an important guide to better regulation in the United States' federal patchwork system. The United States should seek to adopt some of the key portions of the European model instead of continuing to add to the disjointed and fragmented set of laws currently being used. The patchwork quilt of privacy laws that separately limit the use of Americans' information online should give way to a more European-like model of a blanket regulatory system.

Part I of this note examines the background and history of privacy law in the United States. It explores what factors led the U.S. to its current patchwork-system of privacy legislation and what might be preventing the United States from moving towards a more European-model. Part II discusses the underlying attitudes about privacy in the United States versus Europe. This section explains how certain protections and freedoms that citizens from different states value may very well translate into what they choose to protect and what they allow to remain untouched by the state. Part III traces European Union data collection privacy laws and the divergent standards that have materialized in Germany and the United Kingdom. Part IV provides a comparative analysis of the data protection and privacy laws in the European Union and the United States. This section seeks to examine the strengths, weaknesses, and sources of regulation. In addition, this section explores how certain features of the European law can better serve the American people as powerful legal weapons to assert control over their own digital lives. Finally, Part V concludes that implementation of key European laws is possible outside of the European Union. South Africa currently serves as a real-life export of such regulations. This global push towards stricter regulation may help to pressure the United States towards implementing more European regulations.

17. Laura Ybarra, *The E.U. Model as an Adoptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States*, 34 LOY. L.A. INT'L & COMP. L. REV. 267, 271 (2011).

I. THE CONCEPT OF PRIVACY IN GENERAL & INTERNET COMPLICATIONS

All across the Western world, the notion of privacy is seen as an essential element of our humanity, and as such has been described as a value that cuts to our core and somehow "makes life worth living."[18] At the same time, such a fundamental component of our very personhood proves difficult to define. In fact, the United States Courts and Congress have largely avoided defining exactly what the meaning of "privacy" is by adopting a flexible approach to privacy protections that uses voluntary codes of conduct enforced by the Federal Trade Commission mixed with privacy laws that cover certain categories such as health, finance, or education. *Griswold v. Connecticut*, one of the most influential American cases debating the existence of a "right to privacy," did not establish a set body of rights, but rather saw privacy to exist only in the "penumbras" and "emanations" of other Constitutional protections.[19]

This issue has been further complicated with the age of technology and the creation of the Internet. Protecting one's privacy in the "Internet Age" has proven to be immensely difficult, with some believing that with the dawn of social networking, comes the demise of privacy as a "social norm."[20] Others refuse to believe that simply because they utilize the Internet, social media, and email, it somehow bars them from asserting privacy rights.[21]

Privacy law has the elusive task of determining if, and under what conditions, personal information may be discoverable by others. Essentially, privacy law serves as the gatekeeper between the right to be left alone and the right to know. Contemporary technology has made this legal sector far more complicated and has created divisions largely along societal and cultural lines.[22]

The concept of privacy being "all or nothing" is not a notion that may co-exist with the Internet.[23] Internet users, particularly Americans,

---

18. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151, 1153 (2004).

19. Griswold v. Connecticut, 381 U.S. 479, 483-84 (1965).

20. *See* Johnson, *supra* note 1 (discussing how Facebook creator Mark Zuckerberg suggests changing social norms of privacy with creation of social media).

21. *See* Anne Flaherty, *Study Finds Online Privacy Concerns on the Rise*, YAHOO! News (Sept. 5, 2013, 1:42 AM), *available at* http://news.yahoo.com/study-finds-online-privacy-concerns-rise-040211677.html (last visited Apr. 22, 2015) (discussing how Americans are more concerned today about their privacy rights online).

22. *See generally* Whitman, *supra* note 18.

23. Flaherty, *supra* note 21.

are sharing more personal information than ever before.[24] However, they want the power to control what is released and who has access to that information.[25] The Internet remains largely unregulated because of its status as a global enterprise. To further complicate the matter, comfort levels towards releasing personal information online vary greatly. These comfort levels reflect unmistakable differences amongst societies over what ought to be kept "private."[26]

A key illustration of the conflicting notions towards what is to be kept "private" arose in a 2008 case. Millions of Internet users were able to get a glimpse into the private and disreputable sex life of Max Mosley, the then head of Formula One racing, when a British tabloid released the secretly captured videos of Mosley engaging in various sexual escapades with several prostitutes.[27] Mosley successfully sued the British tabloid for the "breach of his privacy" but in today's digital age, removing the tapes from the Internet completely proved more difficult than winning the suit. Luckily for Mosley, European privacy laws place a high value on individual's dignity. This value is seen to be so important that European states provide powerful legal tools to the individual that afford him or her the necessary grounds to sue Internet companies, like Google. The laws in Europe could even compel Google to filter out the videos from Internet searches.[28] This is all because the current E.U. Data Protection Directive affords Europeans the right to "object to the processing of any data relating to himself."[29] In fact, a German court has ordered Google to block all search results in Germany that provide links to Mosley's photos.[30] Mosley's case stands to be further strengthened by a privacy law currently under review by the European Commission that affords citizens the "right to be forgotten,"[31]

---

24. *Id.*

25. *Id.*

26. *See* Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J. L. & TECH. 12, 4 (2011).

27. Eugene K. Chow, *Learning From Europe's 'Right to Be Forgotten'*, HUFFINGTON POST (Sept. 9, 2013), *available at* http://www.huffingtonpost.com/eugene-k-chow/learning-from-europes-rigb3891308.html (last visited Apr. 22, 2015).

28. See Mosley v. News Group Newspapers Ltd., [2008] EWHC 1777 (Q.B.).

29. Council Directive 95/46/EC, *supra* note 15.

30. Harro ten Wolde & Nikola Rotscheroth, *German Court Orders Google to Block Max Mosley Sex Pictures*, RUETERS (Jan. 24, 2014, 8:22 AM), *available at* http://www.reuters.com/article/2014/01/24/us-google-germany-court-idUSBREA0N0Y 420140124 (last visited Apr. 22, 2015).

31. Note from the Presidency to the Council on the 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 10227/13 (May 31, 2013), *available at*

which would "allow individuals to force tech companies to delete all the data it has on them." [32]

So why does Mosley have legal recourse in Europe and not in the United States? Why is there such a transatlantic privacy clash? To answer these questions, we look to the basic intuitions that are "shaped by the prevailing legal and social values of the societies in which we live."[33] We must recognize that European and American sensibilities about privacy have grown from a much larger legal and political tradition. It is the contrast between "privacy as an aspect of dignity and privacy as an aspect of liberty."[34]

II. BACKGROUND OF U.S. LAW

A. Patchwork System of Laws

1. Historical Background in American Law

The American system of privacy law "involves a patchwork of federal and state privacy laws that separately govern the use of personal details in spheres like patient billing, motor vehicle records, education and video rental records."[35] Existing federal laws govern the management of personal information online by regulating specific types of entities and specific types of information. For instance, federal law is in charge of regulating the collection, storage, and distribution of data by "consumer reporting agencies,"[36] regulates how federal governmental agencies collect and handle personal data,[37] and requires financial services corporations to implement measures that ensure the security and confidentiality of their customers' personal data.[38] In addition, the federal government has enacted legislation that oversees the protection, use, and handling of personal data that includes individually identifiable health information,[39] education records,[40] and

---

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010227%202013%20INIT (last visited Apr. 22, 2015).

32. Chow, *supra* note 27.

33. Whitman, *supra* note 18, at 1160.

34. *Id.* at 1161.

35. Natasha Singer, *An American Quilt of Privacy Laws, Incomplete*, N.Y. TIMES, (Mar. 30, 2013), *available at* http://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html (last visited Apr. 22, 2015).

36. Fair Credit Reporting Act, 15 U.S.C.A. § 1681 (West 2014).

37. Privacy Act of 1974, 5 U.S.C.A. § 552a (West 2014).

38. Gramm-Leach-Bliley Act, 15 U.S.C.A. §§ 6801-6809 (West 2011).

39. 42 U.S.C.A. § 1320d-2 (West 2010).

consumer reports.[41]

The United States has separate laws that protect the specific content of the information, but there is no law that spells out explicitly how to control or use online data.[42] This method of dealing with privacy concerns is a result of American history and culture. Suspicion of state power and control has always stood at the core of American privacy law policy, and court doctrine continues to see the state as the prime enemy of a citizen's privacy.[43] For American jurisprudence, the starting point to understanding the origins of the right to privacy begins in the late eighteenth century, most notably in the Bill of Rights, with its forceful constraints on state power.[44] More specifically, the concept of "privacy" starts with the Fourth Amendment and the idea of privacy as being protected from unlawful searches and seizures.[45] Therefore, the right to privacy is a right that "inheres in us as free and sovereign political actors, masters in our own houses, which the state is ordinarily forbidden to invade."[46] Over time American judges and legal scholars have connected this protection of physical spaces and bodies from arbitrary government intrusion, to include a much broader sense of deference for safety and dignity that are necessary to ensure the well-being of our democratic society.[47]

The classic statement of this American ideal came in 1886, in the case of *Boyd v. United States*.[48] The Supreme Court decided to forbid the government from seizing the documents of a merchant in a customs case, after issuing a lengthy opinion discussing the "sanctity" of an American home.[49] The Court reasoned, "[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of

40. Family Education Rights and Privacy Act, 20 U.S.C.A § 1232g (West 2013).
41. Fair Credit Reporting Act, 15 U.S.C.A § 1681-1681x (West 2014).
42. Sengupta, *supra* note 4.
43. Whitman, *supra* note 18, at 1211.
44. *Id.* at 1211-12.
45. *Id.*
46. *Id.*
47. *See* City of Ontario v. Quon, 560 U.S. 746, 755-56 (2010) ("The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government."); Kyllo v. United States, 533 U.S. 27, 31 ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("They [the Framers] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be left alone—the most comprehensive of rights, and the right most valued by civilized men.").
48. Boyd v. United States, 116 U.S. 616 (1886).
49. *Id.* at 625-26.

the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offence."[50] *Boyd*'s fundamental understanding of privacy rights as protecting the "sanctity of the home" have survived generations and continues to be relevant today.[51]

One of the more influential and widely cited articles on the issue of privacy is Samuel Warren and Louis Brandeis' *The Right to Privacy*, published in 1890.[52] The arrival of photography as commonplace in American culture prompted Warren and Brandeis to write the piece, to "warn of the dangers of displaying private family wedding pictures in the pages of every newspaper."[53] Warren and Brandeis specifically emphasized the right to keep personal information outside of the public domain.[54] Although written over 123 years ago, this article still serves as an important dimension to the discussion as it was written in response to the author's own changing technology. Warren and Brandeis' work laid the foundation for the common law development of privacy during most of the twentieth century, and gave rise to the four primary tort causes of action that seek to limit the individual's invasion of privacy as a "right to be left alone."[55] These common law tort actions may be brought by placing someone in a false light, public disclosure of private facts, the intrusion upon a person's seclusion, or the appropriation of a person's name or likeness.[56]

2. FTC Regulation of Online Privacy

Today, the Federal Trade Commission ("FTC") is the leading regulatory agency controlling issues of online privacy.[57] Congress

---

50. *Id.* at 630.

51. Whitman, *supra* note 18, at 1213.

52. *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

53. Sengupta, *supra* note, at 4; Warren & Brandeis, *supra* note 52.

54. *E.g.*, Warren & Brandeis, *supra* note 52, at 198 ("The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.").

55. Whitman, *supra* note 18, at 1208; *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (2010), U.S. DEP'T COM., NAT'L TELECOMM. & INFO. ADMIN. 10, *available at* http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework (last visited Apr. 22, 2015) [hereinafter U.S. DEP'T COM. INTERNET POLICY TASK FORCE].

56. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

57. Michael D. Scott, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN L. REV. 127, 128 (2008).

created the FTC in 1914 in an effort to halt unfair methods of competition arising in the commercial sector.[58] Upon its creation, Congress granted the FTC a tremendous amount of power.[59] Beginning in 1938, the FTC has been the agency charged with preventing corporations from using "unfair or deceptive acts or practices in or affecting commerce" spelled out in Section 45 of the Federal Trade Commission Act.[60] Courts have treated the FTC's decisions with a considerable amount of deference, thereby allowing the FTC to hold a quasi-legislative power to enact its own regulations.[61] However, the FTC has placed limitations on its own regulatory power.[62] Specifically with online privacy concerns, the FTC admits that it "lacks the authority to require firms to adopt information practice policies or abide by the fair information practice principles on their websites, or portions of their websites, not directed at children."[63] The main source of concern stems from the fact that the FTC appears to be limited to enforcing whatever a particular company promises, and most companies are under no legal obligation to make any promises regarding how they collect or use personal data online.[64] In its 2012 report on how to better protect consumer privacy, the FTC suggested that more regulation of online privacy is needed and it is up to Congress to provide such regulation.[65]

Despite its own concern for lack of power, the FTC does in fact bring complaints against companies that violate their established and published privacy policies.[66] In 2010, the FTC filed its first security case against a social networking site.[67] The FTC alleged that social media giant Twitter failed "to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information

---

58. *About the Federal Trade Commission*, FED. TRADE COMM'N, *available at* http://www.ftc.gov/ftc/about.shtm (last visited Apr. 22, 2015).

59. *See id.*

60. *See* Fed. Trade Comm'n Act, 15 U.S.C. §§ 41-58 (2000).

61. *See* Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation,* 69 FORDHAM L. REV. 1305, 1321 (2001).

62. *See* Ybarra, *supra* note 17, at 272.

63. Sovern, *supra* note 61, at 1324.

64. *See generally A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July 2008), *available at* http://www.ftc.gov/ogc/brfovrvw.shtm (last visited Apr. 22, 2015).

65. *See Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers,* FED. TRADE COMM'N (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (last visited Apr. 22, 2015).

66. *See* Scott, *supra* note 57, at 129.

67. *See* In the Matter of Twitter, Inc., 151 F.T.C. 162 (2011).

and honor the privacy choices exercised by its users in designating certain tweets as nonpublic."[68] The security breach by Twitter resulted in two incidents where impostors were able to reset account passwords and access private account information.[69] In one of these instances, the unauthorized user was able to gain access to then-presidential candidate Barack Obama's account and tweet to his over 150,000 followers about a chance to win $500 worth of gasoline.[70] The complaint resulted in an agreement by Twitter to "strengthen its non-public user information and further agreed to [undergo] third-party assessments of its privacy procedures."[71] This case is only one of a limited number of FTC cases brought against social media sites, and serves to underscore the fact that the FTC is hesitant to provide stronger regulation of online privacy through bringing forth more litigation.[72]

Director of the FTC's Bureau of Consumer Protection, David Vladeck, made a statement in 2010 affirming the agency's commitment to protecting consumers through bringing litigation to those companies that may threaten to undermine their personal data.[73] Vladeck stated,

"When a company promises consumers that their personal information is secure, it must live up to that promise. . . . [A] company that allows consumers to designate their information as private must use reasonable security to uphold such designations. Consumers who use social networking sites may choose to share some information with others, but they still have a right to expect that their personal information will be kept private and secure."[74]

3. Sporadic State Regulation

Individual states have provided constitutional privacy rights, however these rights have not been focused on protecting informational privacy.[75] The sporadic nature of regulation, both on the state and federal levels, results in the recognition of only the most serious attacks against privacy interests. Informational privacy issues are regularly

68. *Id.* at 166.
69. *Id.* at 167-68.
70. *Id.* at 168.
71. Ybarra, *supra* note 17, at 273.
72. Sovern, *supra* note 61, at 1321.
73. Press Release, Fed. Trade Comm'n, Twitter Settles Charges That it Failed to Protect Consumers' Personal Information: Company Will Establish Independently Audited Information Security Program, (June 24, 2010), *available at* http://www.ftc.gov/opa/2010/06/twitter.shtm (last visited Apr. 22, 2015).
74. *Id.*
75. Prosser, *supra* note 56.

reviewed under common law privacy torts.[76] Under common law doctrine, a cause of action may be brought by: (a) the placement of someone in a false light, (b) the public disclosure of private information, (c) the interference upon a person's seclusion, or the (d) misappropriation of a person's name or likeliness.[77] There has been a division between state courts about whether informational privacy should extend so far as to comfortably fit within one of these causes of action.[78]

The case law within the United States tends to suggest that courts are hesitant to extend informational privacy protection to fit within one of these four categories.[79] The State of New Jersey, for example, in *State v. Reid*, recognized an individual's reasonable expectation of privacy in the possible disclosure of Internet Service Provider (ISP) records.[80] However, the court stressed the importance in the case that the government was the primary actor in the privacy intrusion.[81] It is very possible that the outcome might have been different if this was not the case. It is likely that state action proved to be an important point in the case holding because of the historical distrust in the United States of possible government intrusion into the lives of its citizens.

In fact, a Pennsylvania court reached an entirely different decision where the primary "offender" was a private actor. In *Boring v. Google, Inc.*, the court found that the images taken of the plaintiff's home from Google Street View did not rise to the level a privacy invasion or an intrusion upon an individual's right to seclusion.[82] The court reasoned that the photos taken by Google were less intrusive than a person knocking on the front door; therefore, the plaintiffs did not suffer any significant injury.[83] What is interesting to note is the fact that Google paid the plaintiffs one dollar in nominal damages when the company entered a consent judgment for trespassing.[84] This judgment stopped higher courts from further investigating the issue of privacy.

These differing outcomes serve as examples of the widespread

---

76. *Id.*
77. *Id.* at 389.
78. Sovern, *supra* note 61, at 1317.
79. *See* Boring v. Google Inc., 362 F. App'x 273, 278-79 (3d. Cir. 2010).
80. State v. Reid, 194 N.J. 386, 388 (2008).
81. *See id.*
82. *Boring*, 362 F. App'x 273 at 278-79.
83. *Id.*
84. Defendant Google Inc.'s Response to Plaintiff's Motion to Stay Pending Petition for Writ of Certiorari from the United States Supreme Court, Boring v Google Inc., No. 08-cv-694 (ARH) (W.D.Pa. 2009), 2010 WL 3445457.

incoherence of decisions dealing with informational privacy cases. It is clear that the courts are focusing very narrowly upon particular issues within the cases, rather than seeking to provide any cohesiveness to establish a set of uniform privacy laws in the United States. The current method taken by courts to examine possible privacy breaches on a case-by-case basis is not ideal for online privacy control. Citizens across the United States have attempted to bring cases before the court in an effort to push for more regulation of the treatment of personal information. However, the existing self-regulating model, claimed by the FTC to be the "least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology" continues to be the most common practice used at the federal and state levels.[85] Therefore, instead of providing citizens with blanket legislation that can provide greater protection of data collection practices, the states and federal governments have been focused on singular practices and sporadic regulation.

III. DIVERGENT NOTIONS OF PRIVACY

Although in many ways the United States and Western European countries are culturally similar, these states are showing very different attitudes towards data protection and privacy online. Every country in the European Union has a privacy law, while the United States remains a firm holdout.[86] In the U.S., we have laws that protect data covering everything from our health and financial records, to the movies we buy online. However, there is no single law that addresses exactly who controls and uses personal data online.[87] The American system may be seen more as a "patchwork of federal and state privacy laws" that govern separate spheres, while the European system has "one blanket data protection directive" that lays out the rules, no matter what the particular sector.[88] For now, European laws and U.S. laws are operating on very different speeds. However, with globalization and the ease of

85. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST L. REV. 587, 600 (2007).

86. Press Release, Eur. Comm'n, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses (Jan. 25, 2012), *available at* http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (last visited Apr. 22, 2015).

87. *See* Sengupta, *supra* note 4 (discussing how Europeans feel about the American perspective on online privacy and the concern over American companies and their control over our digital lives).

88. Singer, *supra* note 35.

worldwide trade and travel, if "the United States wants to foster trust in American companies operating abroad it has to figure out how to explain its privacy laws on a global stage."[89] As of now, this patchwork of American privacy law is "more of a macramé arrangement—with serious gaps in consumer protection, particularly when it comes to data protection online."[90]

In addition to the speed of legislation, it is important to recognize the speed of innovation. The swiftness of progression with regards to the Internet and technology adds to the difficulty of regulating online privacy. While the law has traditionally lagged behind technology, favoring stability and certainty, this comes at a price when technology is evolving so rapidly there is no law to regulate it. This is another area that Europe seems to have recognized as "Europe has forged ahead with its project to modernize data protection."[91] This difference in action can largely be attributed to the difference in thinking about the principle of privacy more generally.[92]

A. Europeans and Personal Dignity

To Europeans, privacy protections fundamentally serve to protect the right to "respect and personal dignity."[93] The core value of European privacy protection seeks to safeguard the "right to one's image, name, and reputation."[94] For Europeans, "dignity, honor, and the right to private life" are among the most important fundamental rights of a human being, and are not to be infringed upon.[95] Europe's legal system sees privacy, regardless of its context, as a core democratic value that must be vehemently protected and not left to market forces to control.[96] Europeans seek to foster the right to guarantee that a person's image to the rest of society is how they wish to be seen. Privacy in Europe is the right to "be shielded against unwanted public exposure—to be spared embarrassment or humiliation."[97] The primary enemy to

89. *Id.*
90. *Id.*
91. *Id.*
92. *See* Chow, *supra* note 27; Newell, *supra* note 26, at 3; Whitman, *supra* note 18, at 1155.
93. Whitman, *supra* note 18, at 1161.
94. *Id.*
95. Chow, *supra* note 27; *see* Whitman, *supra* note 18, at 1155.
96. Joel R. Reidenberg, *Should the U.S. Adopt European-Style Data-Privacy Protections?*, WALL ST. J. (Mar. 8, 2013), *available at* http://online.wsj.com/news/articles/SB10001424127887324338604578328393797127094 (last visited Apr. 22, 2015).
97. Whitman, *supra* note 18, at 1161.

this right is the media, which is constantly threatening to broadcast distasteful information about people in ways that may severely undermine a person's public dignity.[98]

B. Americans and Liberty

American privacy law, on the other hand, is based primarily on the "political value of liberty from government intrusion and sovereignty within the home, rather than public image or social dignity."[99] At its core, the American right to privacy is very much the same as it was at the founding of the nation, "the right to be free from state intrusions, especially in one's own home."[100] American law also values the right to control access to and the distribution of personal information.[101] The prime danger to Americans is that the "sanctity of [our] home[s]", using the language of a leading nineteenth-century Supreme Court ruling on privacy law, will be breached by governmental actors.[102] There is very little concern towards the media's potential to infringe on a person's privacy, but rather the worry focuses on maintaining private autonomy within our own homes.[103] This value is often at odds between the right of free speech and individual rights. The American law focus on individual liberty to control personal information seeks to "allow the individual to determine which information to keep private and which information to release into the public domain."[104] However, American laws frequently prioritize free speech at the expense of individual rights. Mug shots are a prime example, as they are considered public information. This gives rise to numerous websites solely dedicated to publishing mug shots, which publicly shame those shown, regardless of their guilt or innocence, and the First Amendment protects such publication.[105] In contrast, in the United Kingdom, the High Court has ruled that the police must destroy mugshots taken of innocent people.[106] The High Court held that retaining photographs of suspects who were

98. *Id.*

99. Newell *supra* note 26, at 10.

100. Whitman *supra* note 18, at 1161.

101. Newell *supra* note 26, at 10.

102. Boyd v. United States, 116 U.S. 616, 630 (1886); *see also* Whitman, *supra* note 18, at 1162.

103. Whitman, *supra* note 18, at 1162.

104. Newell, *supra* note 26, at 10.

105. Chow, *supra* note 27.

106. Rebecca Camber, *Police Forced to Destroy All Mugshots of Innocents: Schoolboy's Landmark Legal Victory*, UK DAILY MAIL (June 22, 2012, 22:42 GMT), *available at* http://www.dailymail.co.uk/news/article-2163219/Police-forced-destroy-mugshots-innocents-Schoolboys-landmark-legal-victory.html (last visited Apr. 22, 2015).

never charged was a breach of their human rights.[107]

C. Liberty and Dignity Diverge

It is important to note that the distinction between liberty and dignity is not black and white. But this lack of a solid separation can be helpful in creating a more ideal contemporary notion of what is reasonable to protect online. Privacy online should have a healthy respect for control and liberty, while also balancing an essential recognition of the benefits of protecting human dignity.[108] Therefore, American law could greatly benefit from the underlying principle of the "right to be forgotten" dignity from European thinking.[109] When considering the implementation of the "right to be forgotten" in America, the question should not be whether individuals like Max Mosley should be afforded the capability to compel search engines to filter out undesirable content, but rather why it takes a high-profile lawsuit before individuals are given a voice and control over the status of their online selves.[110] When issues of online reputation arise, the burden of proof is placed on the individual, who is already lacks the ability to say how their personal information is distributed and to whom.[111] High-powered tech companies and governmental agencies constantly parse through mounds of online personal data that reveal information from online shopping habits, location data, to even the very content of our emails.[112] Individuals are left with very little control or recourse of their personal data once they click "I agree," so it comes as no surprise that privacy rights online are continually violated.[113] By beginning to implement more of the European notion of privacy online, Americans could have a powerful legal tool to better control their digital lives.[114]

---

107. *Id.*
108. Newell, *supra* note 26, at 4.
109. Chow, *supra* note 27.
110. *Id.*
111. *Id.*
112. *Id.*
113. *Id.*
114. Chow, *supra* note 27.

IV. PRIVACY LAW'S EVOLUTION IN THE E.U.

A. Basic Principles of the E.U. Data-Protection Regime

The current E.U. data-protection regime is set within a large body of legislation that was adopted by its Council of Ministers on October 24, 1995, entitled "European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" ("E.U. Directive").[115] The E.U. Directive requires its member-states to adopt individual national legislation based on the provisions set within and may be characterized as the product of "over fifty years of Europe's devotion to recognizing, maintaining, restoring, and ensuring personal privacy."[116]

The E.U. Directive sets forth eight principles that oversee the gathering and usage of personal information: purpose limitation, data quality, data security, sensitive data protection, transparency, data transfer, independent oversight, and individual redress.[117] The primary purpose of the directive is to "protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data."[118] Essentially, the E.U. Directive seeks to ensure that personal data within the European Union cannot be handled without the individual's permission, unless the processing of such information is either necessary to perform a contract between the entities, or falls within a set exception.[119]

The European Data Protection Supervisor ("EDPS") monitors the handling of personal data within the European Union.[120] The EDPS also serves as an advisor on policies and pieces of legislation that affect privacy in the European Union, as well as works in cooperation with other data-protection authorities to promote consistency in data protection throughout the entire European Union.[121] This agency is an independent entity that was created by the European Parliament and Commission and has broad authority regarding data collection, and

---

115. Council Directive 95/46/EC, *supra* note 15.

116. JON MILLS, PRIVACY: THE LOST RIGHT 82 (2008).

117. *Id.* at 83.

118. *Id.*

119. *Id.*

120. *See generally* EUR. DATA PROTECTION SUPERVISOR, *available at* https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS (last visited Apr. 22, 2015).

121. *See Information Brochures 2009*, EUR. DATA PROTECTION SUPERVISOR 5, *available at*, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Brochures/Brochure_2009_EN.pdf (last visited Apr. 22, 2015).

therefore has helped to make it an effective enforcement organization.[122]

However, each E.U. member-state has its own data-protection authority, given the powers to recommend, counsel, study, and impose punishments for violations of their data-protection laws.[123] This allowance of member-state independence has resulted in natural differences in policy and enforcement. As long as the E.U. member-state maintains the baseline laws and policies of the E.U. Directive, they are free to choose to adopt additional laws and oversight. Looking to both Germany and the United Kingdom helps to provide an example of the different approaches member-states take in data protection. This difference should be seen as not a weak spot in promoting uniformity, but rather as a way for other entities, like the United States to more successfully adopt such a comprehensive system. For instance, if applied to the United States' federalist system, a slight independence among levels would allow for baseline federal uniformity, while also allowing for more "wiggle room" amongst the states.

B. Germany: The E.U.'s Strictest Data Collection Laws

In both 2009 and 2010, the German government passed a number of amendments to the nation's Federal Data Protection Act.[124] These amendments covered a vast array of data collection issues, from tightening the consent requirements of online users, to limiting the transmission of data to commercial agencies.[125] The amendments also increased fines for any violations of the set law and extended the powers of the supervisory authority.[126]

This tightening of online data security has not been exclusively for German-based entities. Germany has kept a close eye on American technology companies.[127] Specifically, German officials have begun investigations of Google, Facebook, and Apple in how they collect and disperse data.[128] "Facebook is being investigated for collecting data on

122. *Id.* at 4.

123. *Id.* at 6.

124. *See* Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, BGBL. I at 2814, *available at* http://www.gesetze-im-internet.de/englischbdsg/ (last visited Apr. 22, 2015).

125. *See generally id.*

126. *Id.*

127. Kevin J. O'Brien, *Despite Privacy Inquiries, Germans Flock to Google, Facebook and Apple*, N.Y. Times (July 11, 2010), *available at* http://www.nytimes.com/2010/ 07/12/technology/12disconnect.html (last visited Apr. 22, 2015).

128. *Id.*

non-Facebook users," whose information was pulled from the mailing lists of active users.[129] Google is under watch for having "errantly collected personal Internet information" during the research phase of its Street View mapping service.[130] And Apple is expected to explain exactly what kind of information it stores about its users and for how long a period of time.[131] It is clear that Germany favors a stricter punitive system, which serves to set out clear guidelines to ensure that those who may violate the law are aware of the consequences.[132]

C. United Kingdom: Least Stringent Data Collection Laws in the E.U.

Alternatively, the United Kingdom has taken a more relaxed approach to privacy protections compared to the German system. In fact, there has been concern among the European Union that the United Kingdom's approach may, at times, not be compliant with E.U. Directives. A 2009 European Commission Union ("E.C.") report maintained it position that the United Kingdom is "failing to comply with EU rules protecting the confidentiality of electronic communications."[133] Citing a lack of an independent and central national authority to oversee the possible interception of communications, the report urged U.K. authorities to change their national laws to ensure complete compliance with the safeguards set out in E.U. law, concerning the right of all E.U. member state citizens to confidentiality of electronic communications.[134] Most recently in September 2013, the United Kingdom has been accused of trying to "impede data protection reforms that would make it more difficult for spy agencies to get hold of material online."[135] Broadly speaking, the apprehension in the United Kingdom is the transfer of more power from Westminster to Brussels.[136] More precisely, the U.K. government is concerned over enforcement.[137] British officials are worried that by have a zero-tolerance policy with privacy intrusions and not leaving

129. *Id.*

130. *Id.*

131. *Id.*

132. Philip Oltermann, *Britain Accused of Trying to Impede EU Data Protection Law*, GUARDIAN, (Sept. 27, 2013), *available at* http://www.theguardian.com/technology/2013/sep/27/britain-eu-data-protection-law (last visited Apr. 22, 2015).

133. *Telecoms: Commission Steps Up UK Legal Action Over Privacy and Data Protection*, EUROPEAN COMM'N (Oct. 29, 2009), *available at* http://europa.eu/rapid/press-release_IP-09-1626_en.htm?locale=en (last visited Apr. 22, 2015).

134. *Id.*

135. Oltermann, *supra* note 132.

136. *Id.*

137. *Id.*

room for possible mistakes, enforcers of the law will be forced to punish even the smallest of offenses, perhaps mistakenly made.[138] This concern has been articulated by a U.K. information commissioner: "If you have inflexible regulation, you overclaim and lose authority. Less is more."[139]

Despite the difference in approaches to regulating privacy between the United Kingdom and Germany, an ever-growing number of their citizens are using a litany of social media sites and online resources.[140] These differences highlight a split that many European nations are experiencing with how to properly draft legislation that adequately reconciles the competing interests of data protection laws, technology companies' push to enter the European market, and consumer attitudes towards privacy in a culture where social media reigns supreme.[141]

V. COMPARING DATA COLLECTION PRIVACY LAWS IN THE UNITED STATES AND EUROPEAN UNION

The United States government is also struggling to come to an agreement on whether to adopt stricter data protection laws. In February 2012, the Obama Administration proposed a "Consumer Privacy Bill of Rights,"[142] but there has been little traction in Congress.[143] Those who continue to "favor industry self-regulation and agreements between Internet companies and their users" are often led by advertising lobbyists and consumer advocates alike.[144] Although, there are others that believe that the U.S. government's entrustment of the Internet industry to police itself has actually created a situation where consumers are left with little control over their own personal data or recourse in the event of a privacy invasion.[145] And this camp is gaining traction. More and more Americans see their representatives are more

138. *Id.*

139. *Id.*

140. O'Brien, *supra* note 127.

141. Ybarra, *supra* note 18, at 267-71.

142. Press Release, Office of the Press Sec'y, Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights (Feb. 23, 2012) (on file with author).

143. Alex Byers, *White House Pursues Online Privacy Bill Amid NSA Efforts*, POLITICO (Oct. 7, 2013, 5:03 AM), *available at* http://www.politico.com/story/2013/10/white-house-online-privacy-bill-nsa-efforts-97897.html (last visited Apr. 22, 2015).

144. *Id.*

145. Reidenberg, *supra* note 96.

interested in protecting commerce than the consumer. This commercial interest is often cloaked in the stance that strict regulation of information among citizens will inevitably lead to the situation that Chinese citizens face, with barriers to Internet-access called the "Great Firewall."[146] This fear has been described as the belief that such rigorous standards and disclosure in Internet policy-making would create countries that could best be seen as "series of walled gardens with governments holding the keys to locked gates."[147] Often U.S. lawmakers cite the importance of free speech and individual autonomy in keeping with the status quo of Internet self-regulation.

Freedom of expression is an extremely valuable and important right to protect because it works to ensure a stable democratic society. At the same time, privacy is also valuable and vital protection, because it works to ensure personal health and flourishing. Therefore, the two million dollar questions are, at what point does speech and free expression violate informational privacy, and what personal information is essential to ensure democratic stability?[148] While American history has long publicized the individual as the pillar of society, it is European law that has a much clearer respect for the individual, at least in terms of privacy protection.[149] This is evidenced by a long history in Europe of prioritizing people over photographers, newspapers, and technology companies.[150] So why do such similar cultures and sets of values seem to stray from one another in the realm of online privacy? To best understand the difference in mentality and priority between the United States and Europe is to take two instances of similar circumstances and compare.

A. Princess Caroline of Monaco

Princess Caroline of Monaco battled a long fight in multiple European courts in seeking to protect her right to prevent the publication of various unauthorized photographs.[151] The photos

146. Danny Hakim, *Europe Aims to Regulate the Cloud*, N.Y. TIMES (Oct. 6, 2013), *available at* http://www.nytimes.com/2013/10/07/business/international/europe-aims-to-regulate-the-cloud.html?pagewanted=all (last visited Apr. 22, 2015).

147. *Id.*

148. ADAM MOORE, PRIVACY RIGHTS: MORAL AND LEGAL FOUNDATIONS, 144-45 (2006).

149. Chow, *supra* note 27.

150. *Id.*

151. Von Hannover v. Germany, 294 Eur. Ct. H.R. at 25 (2004) (Section 25 of the European Court of Human Rights opinion is a reproduction of the relevant portions of the decision by the German Federal Constitutional Court).

included images of her and her children engaging in various private activities. With the photos of her children, the German Federal Constitutional Court (Bundesverfassungsgericht) found that a parent's relationship with their children warranted more privacy protection.[152] However, the images of just Princess Caroline shopping and sunbathing were found not to necessitate further protection because Princess Caroline is a public figure,[153] and the photographs showed her in public places.[154]

She appealed to the European Court of Human Rights, which found that the German court's decision violated her right to privacy under the European Convention on Human Rights.[155] The court balanced Princess Caroline's Article 8 "right to respect her private life" against the Article 10 "right of freedom of expression."[156] What ultimately tipped the scales in favor of Princess Caroline and her right to privacy was the substance of the photographs. The court categorized the pictures as portraying Caroline in "activities of purely private nature such as engaging in sport, out walking, leaving a restaurant or on holiday."[157] Because these photos did not "contribute to a debate of general public interest" and Princess Caroline performed no official function, these images were only related to her private life and fell within the bounds of protection.[158] The court argued, "photos appearing in the tabloid press are often taken in a climate of continual harassment which induces in the person concerned a very strong sense of intrusion into their private life or even of persecution."[159]

It is important to note that the photographs in this case would almost certainly have fallen under the protection of the First Amendment if this case were heard in the United States. What is interesting here is the European court's inclination to differentiate between the types of subject matter and content that could be seen to fall under public interest and what does not. It is clear that American courts prefer to permit speech and err on the side of "newsworthiness" when faced with a First Amendment case, which often results in the loss

152. *Id.*

153. German case law refers to a "figure of contemporary society '*par excellence.*'" *Id.* para. 18.

154. *Id.* para. 25.

155. MILLS, *supra* note 116, at 100.

156. *Id.*

157. Von Hannover v. Germany, 294 Eur. Ct. H.R. para. 25 (2004).

158. *Id.* at 65; *see also* MILLS, *supra* note 116, at 100.

159. Von Hannover v. Germany, 294 Eur. Ct. H.R. at 59 (2004).

of privacy rights.[160]

B. Sipple v. San Francisco Chronicle, Inc.

In contrast, in 1975, the California Supreme Court upheld the right of journalists to publicly out Oliver Sipple as a gay man after he stopped an assassination attempt on President Gerald Ford. While most of the media outlets celebrated Sipple as a hero in protecting President Ford, a reporter discovered Sipple was a homosexual, a fact that his family was not aware of.[161] Despite Sipple's repeated requests to the media to keep his sexual orientation private, the court reasoned that Sipple was a public figure, thereby surrendering many of his privacy protections.[162] The court subsequently denied his motion to suppress and a hero's sexuality quickly became part of the news headlines.[163]

The information in this case can be split into two categories. The first deals with the facts like the assassination attempt, Sipple's duties as a secret service agent, and his actions in removing the President from a dangerous situation as appropriate to publish and circulate.[164] The second category deals with the sensitive information about the citizen-hero, like his sexuality, home address, medical history, or favorite hangout spot.[165] These pieces of information are entirely "personal" and are by no means relevant in helping to maintain a stable democratic institution or more open society. Sipple's outing quickly led to his parent's discovery that he was gay, which ultimately led to ostracization from his family, depression, and a battle with alcoholism.[166] In Sipple's case, by upholding such a rigid protection in favor of the freedom of expression, Sipple was neither afforded the American "right to be left alone" nor the European right to "dignity, honor, and the right to private life."[167]

It has become clear that in matters concerning one's reputation online or in the media, the burden of proof is placed firmly on the individual. This can prove to be extremely difficult as the individual is already at a disadvantage compared to the tech giants and media moguls. Individuals have little to say about how their personal

160. MILLS, *supra* note 116, at 100.
161. MOORE, *supra* note 137 at 147.
162. Chow, *supra* note 27.
163. Sipple v. Chronicle Publ'g Co., 154 Cal. App. 3d 1040, 1044-45 (Ct. App. 1984).
164. MOORE, *supra* note 148, at 148.
165. *Id.*
166. Chow, *supra* note 27.
167. *Id.*

information is collected or distributed to the rest of the world. However, if more courts begin to follow the pattern of analysis from Princess Caroline's case, the individual will be able to assert more control over personal data and information, giving Americans and Europeans alike a powerful legal weapon to better assert control over our own digital identities.

VI. WHETHER OR NOT THE E.U. SYSTEM WOULD WORK IN THE U.S.

A. Where Should the Law Go in the Future?

Companies are watching us. They want to know what sites we visit on the Internet, what we choose to buy, and as much personal information as they can gather about us. This is all in the hopes of targeting their own marketing campaigns and sending online users specific offers based on our online personas. So if companies are watching us, who's watching over them? Who is making sure they don't misuse personal data or break promises they make to consumers about handling their private information? In the United States, the answer is largely no one. Self-regulation seems to be the name of the game. But this entrustment to the industry to regulate itself has created a state where the ordinary individual has little control over their own online information and even less control over remedies they may exercise when their privacy has been raided. However, as we have seen in Europe, there are strict regulations about what companies can and cannot do in terms of data collection, and governments are pushing to make these already rigorous rules even more rigorous. The United States should look to this European model in helping to expand our limited legal rights seeking to protect us against online tracking and profiling. There are a number of qualities that the European system possesses that the American model can greatly benefit from imitating.

First and foremost, the European system recognizes privacy, regardless of the subject matter, as a core democratic value that must be vehemently protected. It must not be left to market-forces to protect; the State must step up to the plate to protect the individual against the industry. Second, information today has immense value so it only makes sense that good business practice includes knowing what information a company holds, how they store it, and making sure its used properly. Strict and far-reaching privacy standards seen in the European Union serve to encourage companies to adopt practices that respect the power of information and ensure they adopt practices that

protect the collection and storage of information, or risk the punishment for misconduct. Third is the fact that in Europe, individuals have legal recourse and action to take when their privacy rights have been violated. In the U.S., remedies only exist in small sectors of privacy rights. For instance, if a doctor reveals a patient's medical condition, the patient would be permitted to sue under the health-information privacy law, but if a website was to disclose the very same information, the website user would have no claim.[168] This lack of consistency leaves major gaps in privacy protection and greatly undermines public trust in the protection of their online activity. Fourth, it is very important to have oversight in the enforcement of privacy rules. The independent nature of the oversight board helps to ensure privacy compliance in a constantly changing and complex online world. This independent board exists in the European Union, yet remains without a counterpart here in the United States.

Some critics assert that legislators and officials in Washington cannot be trusted with developing complex privacy law and it should be left to market-forces to correct the intrinsic flaws in the current system.[169] While this may have been true in the past, privacy has and continues to garner bipartisan support. Particularly in light of recent online privacy scandals, like Edward Snowden's National Security Agency leaks about the existence of American spies or the Target Company's credit card information breach, more and more Americans are seeking more legal protections online.[170] Our current system of self-regulation is not the only viable option for the United States. It is possible for the U.S. to adopt important practices currently being done in Europe. In fact, lawmakers in South Africa are doing just that.

B. South Africa Implementing European-like Laws

For those who assert that comprehensive laws on privacy protection can only be successful in Europe, South Africa serves as an interesting counter example. The effort in Europe to adopt the world's strongest data protection laws has drawn international attention. Often new regulation proposals are motivated by the desire to rein in the unregulated data collection of powerful social media companies like Google, Facebook, and Twitter. Companies in the United States, like

168. Reidenberg & Davenport, *supra* note 96.

169. *Id.*

170. Adam Blenford & Christine Jeavans, *After Snowden: How Vulnerable is the Internet?* BBC NEWS (Jan. 27, 2014), *available at* http://www.bbc.co.uk/news/technology-25832341 (last visited Jan. 30, 2015).

Exxon Mobil, Amway, Aon, and Procter & Gamble, remain interested in the discussions going on in Europe about stronger and stronger rights for consumers.[171] Often they send representatives to conferences and governmental body meetings where regulations are debated on. But these multinational companies are not the only ones watching what is happening in Europe, other countries are watching as well. In fact, lawmakers in South Africa have been so interested in the European regulations that they have decided to replicate it.

The South African Parliament passed the "Protection of Personal Information Act" on August 22, 2013 and it officially became law on November 26, 2013.[172] This Act essentially regulates how anyone who processes and is exposed to personal information must handle that information, and ensure that that information is kept safe and secure.[173] The Protection of Personal Information Act has taken over eight years to complete, but the final result has been largely seen as a solid piece of legislation.[174] This act represents the country's first comprehensive data protection laws, which are greatly crafted from the E.U.'s rules.[175] Lawmakers hope that this new act will help South Africa become internationally recognized as a nation with impressive data protection standards, thereby attracting businesses to the country.[176]

Although the legislation allows a one-year compliance window, it is already quite clear that this law means business. The rules are strict and deviation means substantial penalties. A party that does not comply with the Act's provisions faces possible prison time and fines up to 10 million Rand.[177] For instance, Zurich Insurance lost an unencrypted back-up disk in South Africa and the mistake cost the company £2.3 million.[178] In addition, the legislation permits individuals to file

171. Kevin J. O'Brien, *Firms Brace for New European Data Privacy Law*, N.Y. TIMES (May 13, 2013), *available at* http://www.nytimes.com/2013/05/14/technology/firms-brace-for-new-european-data-privacy-law.html (last visited Apr. 22, 2015) (Aon is headquartered in London, United Kingdom) [hereinafter *Firms Brace for New European Data Privacy Law*].

172. Hunton & Williams, LLP, *South Africa Passes Comprehensive Personal Data Protection Legislation*, PRIVACY & INFO. SECURITY L. BLOG (Aug. 30, 2013), *available at* https://www.huntonprivacyblog.com/2013/08/articles/south-africa-passes-comprehensive-personal-data-protection-legislation/ (last visited Apr. 22, 2015).

173. Lucien Pierce, *Protection of Personal Information Act: Are You Compliant?*, MAIL & GUARDIAN (Dec. 2, 2013, 1:15 PM), *available at* http://mg.co.za/article/2013-12-02-protection-of-personal-information-act-are-you-compliant/ (last visited Apr. 22, 2015).

174. *Id.*

175. *Firms Brace for New European Data Privacy Law, supra* note 171.

176. *Id.*

177. Pierce, *supra* note 173.

178. *Id.*

separate civil complaints, so offenders face additional financial losses on top of whatever fines are imposed. It is clear that there is a global "expectation that data protection laws around the world are going to become more stringent, and Europe is leading the way."[179]

This piece of legislation serves as an important example of the viability, success, and influence that the European model of data protection has on an international scale. Stringent data protection is not just something that is important to Europeans, it is important on a global scale. There is no doubt that the world will be watching South Africa and monitoring the success of this new Act. Its success may serve as an important model of the viability of the European perspective outside of the region. In addition, the success may add further pressure to the United States and its lawmakers for similar changes. If it is one thing that the United States hates, it is the feeling of being behind the rest. If the South African government can show this law to be successful, American lawmakers will certainly feel the pressure to join the club.

CONCLUSION

"Personal data is the oil that greases the Internet"[180] and each one of us sits on a vast reserve of this oil. It's the data that we share each and every day, the names, addresses, pictures, and even our exact locations, with our GPS and Internet equipped smartphones.[181] This information helps multi-million dollar companies target their advertising and discern our personal opinions and desires based on what we choose to post online.[182] This information translates into millions of dollars for companies. But there is a price for us, the consumer. The data that we post about our lives and desires are collected, dissected, and preserved, often for a very long time, by numerous companies.

Personal data is extremely valuable. It is because of its immense value to a great deal of companies that we will no doubt see resistance from the business sector if and when any new data collection laws are proposed here in the United States. In fact, we are already seeing companies prepare themselves for such an occurrence. In January 2011, it was reported that Facebook beefed up its Washington presence as the Federal Trade Commission and Department of Commerce began to consider additional and clearer safeguards that Internet companies must

179. *Firms Brace for New European Data Privacy Law, supra* note 171
180. Sengupta, *supra* note 4.
181. *Id.*
182. *Id.*

begin to use when collecting user data.[183] Current laws allow companies to be vague about their privacy policies and data collection, and many do not wish to change such policies. Lawmakers have allowed this to happen because the business sector is given immense latitude because the government does not wish to stifle innovation.[184] But this resistance should not stop us, and in fact it is not.

According to a survey conducted in July 2013 by the Pew Internet Center, most Americans said that they believed current laws on online privacy protections were inadequate.[185] Many of those surveyed said they did what they could to protect themselves, namely clearing browsing histories, deleting social media posts, or utilizing encryption tools.[186] And while Congress has largely stalled in its efforts to protect the public, State lawmakers are responding to the concerns of their constituents. For instance, over the last couple of years, ten states have passed laws restricting employers from requiring access to their employees' social media accounts.[187] It is clear that State legislatures across the United States are facing growing worries about the collection and use of personal data, and many have swiftly proposed a series of privacy laws from requiring police to obtain warrants to track cellphone locations to how schools can collect student data from their online usage.[188] "Congress is obviously not interested in updating those things or protecting privacy," said Jonathan Strickland, a Republican state representative in Texas.[189] "If they're not going to do it, states have to do it."[190] And with the recent reports on eavesdropping by the federal government, the issue of digital privacy is becoming more and more pressing for many citizens. With these concerns becoming increasingly widespread amongst the states, it is only a matter of time before the federal government has no choice but to take notice.

As the United States adopts new data protection law, it may look to the European Union as an adoptable model. U.S. citizens are "becoming

---

183. Jon Swartz, *Facebook Changes Its Lobbying Status in Washington,* USA TODAY (Jan. 13, 2011, 10:51 AM), *available at* http://www.usatoday.com/money/industries/technology/2011-01-13-facebook13_CV_N.htm (last visited Apr. 22, 2015).

184. *See* U.S. DEP'T COM. INTERNET POLICY TASK FORCE, *supra* note 55.

185. Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, N. Y. TIMES (Oct. 30, 2013), *available at* http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html (last visited Apr. 22, 2015) [hereinafter Sengupta, *No U.S. Action*].

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. Sengupta, *No U.S. Action*, *supra* note 185.

increasingly wary that their lives are going to be no longer their own," said Georgia state representative John Pezold, "and we have got to protect that."[191] There is no doubt that there are a number of competing factors, such as consumer mindsets and commercial sector interests, that complicate the implementation of new and stronger privacy laws in the United States. However, data collection laws can and must be implemented to provide Americans with broader protections in today's modern digital age.

191. *Id.*