9-1-2011

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

Laura Ybarra
Loyola Law School Los Angeles

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

LAURA YBARRA*

I. INTRODUCTION

In a statement evoking Orwellian images, former Google CEO Eric Schmidt spoke about the possibility of his company improving its search engine: "We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about."[1] In a later television appearance on CNN, the former CEO did little to assuage privacy concerns over Google's Street View map, a service that provides panoramic views from various positions along many streets in the world, when he said: "We drive exactly once. So you can just move, right?"[2] Schmidt's comments underscore not only the pervasiveness of technology but also its implications on an individual's privacy in a technological age. It is this unanticipated ubiquity of technology that has Europeans and Americans alike confronted with the functionality of privacy laws in an age of data collection.

In 2009, Germany passed amendments to the country's Federal

* J.D., Loyola Law School, 2012; B.A., University of Southern California, 2008. My deepest thanks are reserved for my parents for their love and support, and Philip for all his encouragement.

1. Catharine Smith, *Google CEO Eric Schmidt's Most Controversial Quotes About Privacy,* HUFFINGTON POST (Nov. 4, 2010), http://www.huffingtonpost.com/2010/11/04/google-ceo-eric-schmidt-privacy_n_776924.html#s170420.

2. Wilson Rothman, *Don't Like Google Street View? Just Move, Says CEO*, TECHNOLOG ON NBCNEWS.COM TECH (Oct. 25, 2010), http://www.technolog.msnbc.msn.com/technology/technolog/dont-google-street-view-just-move-says-ceo-126480.

Data Protection Act.[3] These amendments covered a broad range of data collection issues including a requirement of notification of data security breaches[4] and changes in data marketing rules.[5] The 2009 amendments also called for increased fines for violations of the law,[6] and expanded the powers of the supervisory authority.[7]

Germany has sparred with American technology companies Apple, Facebook, and Google. The country has launched investigations into how these companies collect and store personal data.[8] For instance, German officials asked Google to turn over data from home wireless networks that were collected while the company compiled information for its Street View map.[9] German data-protection officials launched legal proceedings in August 2010 because of how Facebook handles non-user information.[10] German officials questioned Apple about the duration and the type of personal information the company stores on its iPhone 4.[11]

By contrast, U.K. laws take a more hands-off approach to privacy laws compared to their German counterparts. A 2009 European Commission Union (E.C.) report admonished the United Kingdom (U.K.) about its privacy laws.[12] The E.C. report concluded that the U.K. violated European Union (E.U.) rules by failing to adequately protect its citizens' personal data.[13] The E.C. cited the lack of an independent national authority to supervise interception of communications,[14] and further urged the government to enact laws that ensured safeguards in

3. Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 1, 2002, BGBL. I, last amended by Gesetz [G], Sept. 1, 2009, BGBL. I (Ger.).

4. *Id.* § 42(a), § 33.

5. *Id.* § 30(a), § 28(a), § 32.

6. *Id.* § 43.

7. *Id.* § 23, § 38.

8. Google-Street-View Tours Also Used for Scanning WLAN-Networks, FED. COMMISSIONER FOR DATA PROTECTION & FREEDOM INFO. (Apr. 23, 2010), http://www.bfdi.bund.de/EN/PublicRelations/PressReleases/2010/GoogleWLANScan.html?nn=410214 [hereinafter Commissioner's Press Release]. *See also* Kevin O'Brien, *Despite Privacy Inquiries, Germans Flock to Google, Facebook and Apple*, N.Y. TIMES, July 12, 2010, at B8.

9. Commissioner's Press Release, *supra* note 8; *see also* Kevin O'Brien, *Google Balks at Turning Over Data to Regulators*, N.Y. TIMES, May 28, 2010, at B3.

10. Christopher Lawton & Vanessa Fuhrmans, *Google Rouses Privacy Concerns in Germany—Mapping Service Sparks Debate as Nation Scarred by Authoritarian Past Grapples With Personal Data in Digital Age*, WALL ST. J., Aug. 17, 2010, at B5.

11. *Id.*

12. Press Release, European Union, Telecoms: Commission Steps Up UK Legal Action over Privacy and Personal Data Protection, (Oct. 29, 2009), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626.

13. *Id.*

14. *Id.*

compliance with E.U. laws.[15]

The U.K.'s approach to handling data breaches has differed notably from that of Germany. For instance, as Google gathered data for its Street View map and collected personal information from wireless Internet networks, including passwords and e-mail messages, the company avoided fines in the U.K. merely by promising to take steps to avoid any repetition of what Google described as "inadvertent" incidents.[16] The company also agreed to delete the data it collected and provide training for its employees on privacy issues.[17]

Although the United Kingdom and Germany have taken different approaches to regulating privacy, more and more of their citizens are joining Facebook, searching on Google, and using Apple products.[18] These differences reveal a growing rift between E.U. laws and consumer behavior in a technological society.[19] This split has confronted European countries with a quandary of how to draft legislation that reconciles the competing interests of data protection laws, technology companies' desire to enter the European market, and consumer attitudes towards individual privacy in a culture where technology and social media are ubiquitous.[20]

The United States government is also struggling to adopt stricter data collection privacy laws at the urging of consumer advocates. A draft Internet privacy law was released to the public in May 2010 by Representatives Rick Boucher and Cliff Stearns, members of the House of Representative's Subcommittee on Communications, Technology and the Internet.[21] The draft bill called for privacy notices to be clearly marked on websites and for these notices to include how the information is stored.[22] The proposed bill made distinctions between data that could be used only with the user's consent and data that could be used until the user opted-out.[23] The bill was met with criticism from advertising lobbyists and consumer advocates alike.[24]

---

15. *Id.*

16. Eric Pfanner, *British Agency Says Google Violated Privacy Law*, N.Y. TIMES (Nov. 3, 2010), *available at* http://www.nytimes.com/2010/11/04/technology/04google.html.

17. *Id.*

18. O'Brien, *supra* note 8.

19. *Id.*

20. *See e.g.,* Christopher Lawton, *Google Street View Sparks New German Privacy Code*, WALL ST. J., Sept. 21, 2010, at B4.

21. H.R., 111TH CONG. (Discussion Draft May 3, 2010) [hereinafter Discussion Draft].

22. *Id.* at 9.

23. *Id.* at 12.

24. Diane Bartz, *John McCain, John Kerry Introduce Contentious U.S. Privacy Bill*, REUTERS (Apr. 12, 2011), http://www.reuters.com/article/2011/04/12/us-congress-privacy-

Like Europe, the United States has taken varying approaches to data collection issues. For example, it was reported in October 2010 that the Federal Trade Commission (FTC) was dropping its investigation of the information Google had obtained during preparation for the launch of its Street View mapping service.[25] The investigation ended with Google agreeing to improve its data collection process and provide privacy training for its employees.[26] Nevertheless, Congress took notice after the *Wall Street Journal* reported in October 2010 that Facebook applications, or "apps," were passing on private user information to advertisers.[27] Congressmen Joe Barton and Edward Markey, co-chairmen of the House's Bipartisan Privacy Caucus, sent a letter to Facebook CEO Mark Zuckerberg asking for more details about how the company's applications handle personal data.[28] After receiving a response from Marne Levine, Vice President of Global Public Policy for Facebook,[29] the Congressmen said they wanted to take up the topic when Congress resumed its 2011 session.[30]

This Note will explore whether the European Union's privacy laws could serve as a model for the United States. Currently, U.S. data collection laws are regulated by a patchwork system of state and federal laws and agencies.[31] The E.U.'s 1995 Directive on Data Protection, on the other hand, mandated that each E.U. nation pass national privacy laws and called for the creation of a Data Protection Authority to protect

---

idUSTRE73B59E20110412.

25. Grant Gross, *FTC Closes Investigation into Google's Wi-Fi Snooping*, TECHWORLD, (Oct. 28, 2010), http://www.techworld.com.au/article/365929/ftc_closes_investigation_into_google_wi-fi_snooping/?fp=4&fpid=16.

26. John D. Sutter, *FTC Ends Google 'Street View' Investigation Without Fines*, CNN (Oct. 27, 2010, 1:59 PM), http://www.cnn.com/2010/TECH/web/10/27/ftc.google.investigation/index.html?eref=rss_tech&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+rss%2Fcnn_tech+(RSS%3A+Technology).

27. Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WALL ST. J. (Oct. 18, 2010), http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html; *see also* Letter from Marne Levine, Vice President, Global Public Policy at Facebook, to Edward Markey, Congressman, and Joe Barton, Congressman, Bi-Partisan Privacy Caucus (Oct. 29, 2010) [hereinafter Letter from Marne Levine], *available at* http://Republicans.EnergyCommerce.house.gov/Media/file/Letters/102910_Facebook_Response_Barton_Markey.pdf.

28. Letter from Marne Levine, *supra* note 27.

29. *Id.*

30. *Facebook Responds to Barton, Markey,* HOUSE ENERGY & COM. COMMITTEE (Nov. 3, 2010), http://republicans.energycommerce.house.gov/news/PRArticle.aspx?NewsID=8085.

31. Ken D. Kumayama, *A Right to Pseudonymity*, 51 ARIZ. L. REV. 427, 434 (2009); *see, e.g.*, The Online Privacy Protection Act (OPPA) of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004), Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 201.

citizens' privacy.[32] The E.U. model allows for variation of data collection laws by allowing its member countries to determine their own laws.[33] It is this degree of latitude, however, that has resulted in a disharmony of laws within the European Union.[34]

Part II of this note begins with an overview of current data collection privacy laws in the United States and further analyzes the May 2010 Congressional Internet privacy draft bill. Part III traces E.U. data collection privacy laws and the diverging standards that have emerged in the United Kingdom and Germany. Part IV provides the comparative analysis of data collection privacy laws in the United States and the European Union. This section analyzes the strengths and limitations of the proposed bill, and analyzes which features from the E.U. model would best serve federal legislation in the United States. Finally, Part V concludes that while the E.U. model provides an umbrella legislative system that would improve the patchwork system of current U.S. data collection privacy laws, the United States should strengthen FTC enforcement powers and preempt state laws to avoid the disharmony of the E.U. system.

II. BACKGROUND OF U.S. LAW

A. A Patchwork System of Data Collection Standards

The United States Supreme Court recognized the fundamental right to privacy in the seminal 1965 case *Griswold v. Connecticut*.[35] There, the Court found that the Bill of Rights provided penumbras of privacy as it struck down a law that forbade the use of contraceptives.[36] Scholars have argued that privacy in the United States is based upon the value of liberty.[37] The notion of privacy as a liberty interest has been

32. Council Directive 95/46, arts. 27–28, Oct. 12, 1995, 1995 O.J. (L 281) (EC) [hereinafter Council Directive 95/46], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:EN:PDF.

33. *See, e.g.*, Commission Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, A.4—Germany, final (June 2010) [hereinafter A.4—Germany], *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf.

34. *Compare* Commission Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments: A.6—United Kingdom, EUR. COMM'N (June 2010) [hereinafter A.6—United Kingdom], *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A6_united_kingdom.pdf, *with* A.4—Germany, *supra* note 33.

35. *See* Griswold v. Connecticut, 381 U.S. 479 (1965).

36. *Id.* at 483 (discussing penumbras within the Bill of Rights that create zones of privacy).

37. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113

exhibited in the Court's treatment of several contentious social issues such as abortion[38] and homosexuality.[39] Furthermore, case law in the United States has recognized the right of privacy free from governmental intrusion.[40] While decisional privacy has been protected, informational privacy has yet to receive such broad protection from the Supreme Court.[41] Instead, informational privacy has become rooted in statutory law, common law, agency regulations, and self-regulatory principles.[42]

1. Ineffective FTC Regulation of Online Privacy

Congress formed the FTC in 1914[43] in an effort to stop unfair methods of competition in commerce.[44] With its creation, Congress granted the FTC a large degree of power.[45] Since 1938, the FTC has been empowered to prevent corporations from using "unfair or deceptive acts or practices in or affecting commerce" under Section 45 of the Federal Trade Commission Act.[46] Courts have treated the FTC's decisions with deference, thus allowing the FTC to possess quasi-legislative power to enact regulations.[47]

Today, the FTC is the leading regulating authority of online privacy issues in the United States.[48] However, the FTC has placed limitations upon its own regulatory power. On the issue of online privacy, for example, the FTC noted that it "lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites, or portions of their Web sites, not directed to children."[49] Recently, the FTC conceded that

---

YALE L.J. 1153, 1161 (2004).

38. *See* Roe v. Wade, 410 U.S. 113 (1973).

39. *See* Lawrence v. Texas, 539 U.S. 558 (2003).

40. Kumayama, *supra* note 31, at 435–36.

41. *Id.*

42. *Id.* at 434–35. *See, e.g.,* Fair Credit Reporting Act, 15 U.S.C. § 1681.

43. *About the Federal Trade Commission*, FED. TRADE COMMISSION (Jan 5, 2012), http://www.ftc.gov/ftc/about.shtm.

44. *Id.*

45. *Id.*

46. *See* Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2000), *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2000-title15/pdf/USCODE-2000-title15-chap2-subchapI.pdf.

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

48. 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).

49. Sovern, *supra* note 47, at 1324. *See Twitter Settles Charges That It Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program*, FED. TRADE COMMISSION, (June 24, 2011),

more regulation of online privacy was needed and suggested a universal "Do Not Track" mechanism as a guard for online privacy.[50] The FTC, however, argued that Congress should provide such regulation.[51]

The FTC does, however, bring complaints against companies that violate their published privacy policies.[52] David Vladeck, the director of the FTC's Bureau of Consumer Protection, affirmed that promise in a 2010 statement: "When a company promises consumers that their personal information is secure, it must live up to that promise."[53] In 2010, the FTC brought its first data security case against a social network.[54] In that suit, the FTC alleged that Twitter failed "to provide reasonable and appropriate security to prevent unauthorized access to nonpublic user information and honor the privacy choices exercised by its users."[55] The breach resulted in two incidents where intruders were able to reset account passwords.[56] In one instance, the intruder tweeted from then-presidential candidate Barack Obama's account, offering his followers a chance to win $500 in gasoline.[57] In an agreement with the FTC, Twitter agreed to strengthen its non-public consumer information and further agreed to third-party assessments of its privacy procedures.[58]

In March 2011, Google agreed to settle charges that it violated its own privacy promises to consumers with its launch of Google Buzz.[59] Google agreed to implement a "comprehensive privacy program" and agreed to privacy audits for twenty years.[60] Yet the fact that the FTC has

---

http://www.ftc.gov/opa/2010/06/twitter.shtm.

50. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 4–5 (2012). *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

51. Sovern, *supra* note 47, at 1325.

52. Scott, *supra* note 48, at 129.

53. Press Release, Federal Trade Commission, 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.

54. Complaint, Twitter, Inc., 151 F.T.C. 162 (2011) [hereinafter Twitter Complaint].

55. *Id.* ¶ 11.

56. *Id.* ¶ 12(a).

57. *Id.*

58. Agreement, Twitter, Inc., 151 F.T.C. 162 (2011) [hereinafter Twitter Agreement].

59. Agreement Containing Consent Order, In the Matter of Google Inc., File No. 102 3136, http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf [hereinafter Google Agreement]. The FTC complaint alleged that Google users were not adequately informed that the default setting allowed frequent contacts to be public. Complaint, Google, Inc., File No. 102 3136 (Oct. 24, 2011), http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf. *See also* Press Release, Federal Trade Commission, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://www.ftc.gov/opa/2011/03/google.shtm [hereinafter FTC Press Release].

60. Google Agreement, *supra* note 59, at 4–5.

only brought a limited number of cases against social networking sites is indicative of the agency's hesitance to provide stronger regulation of data collection practices.[61]

2. Sporadic state regulation of privacy rights

States have provided constitutional privacy rights, but these rights have not been focused on informational privacy.[62] Because of the federal and state governments' sporadic regulation of informational privacy, only serious invasions of privacy interests have been recognized.[63] Informational privacy issues are generally analyzed under common law privacy torts.[64] Under common law, an invasion of privacy cause of action could be brought under: (1) the placement of someone in a false light; (2) the public disclosure of private facts; (3) the intrusion upon a person's seclusion or solitude; or (4) appropriation of a person's name or likeness.[65] This approach has caused scholars to debate whether informational privacy should extend so far as to fit within one of these causes of action.[66]

The case law within the United States suggests, however, that courts have not extended informational privacy protection within the invasion of privacy tort.[67] New Jersey, for example, recognized an individual's reasonable expectation of privacy in Internet service provider (ISP) records in the 2008 case *State v. Reid*.[68] There, however, the court focused on the notion of privacy when the government was the actor.[69] It is likely that a different result would have been reached had the actor been a private entity.

Indeed, a Pennsylvania court reached a different decision where the actor was a private entity. In *Boring v. Google, Inc*., the court held that images of the plaintiff's house from Google's Street View did not rise to the level of invasion of privacy or intrusion upon seclusion.[70] There, the court reasoned that the photographs were less intrusive than a knock on the front door, and thus concluded that the plaintiffs did not suffer a substantial injury.[71] In December 2010, however, Google paid

61. Sovern, *supra* note 47, at 1321.
62. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 386–88 (1960).
63. *See* Twitter Complaint, *supra* note 54, ¶ 11; State v. Reid, 945 A.2d 26, 33 (N.J. 2008).
64. Prosser, *supra* note 62, at 389.
65. *Id.*
66. Sovern, *supra* note 47, at 1317–18.
67. *See* Boring v. Google Inc., 362 F. App'x 273, 278–79 (3d Cir. 2010).
68. *See* Reid, *supra* note 63 at 28.
69. *Id.*
70. *See* Boring, *supra* note 67 at 280.
71. *Id.* at 279.

the plaintiffs one dollar in nominal damages when the company entered a consent judgment for trespassing.[72] This judgment prevented higher courts from further analyzing the issue of privacy.

Because of the limitations of recovery for plaintiffs under the common law system, many states have enacted legislation to provide its citizens with far greater informational privacy protection.[73] These laws, however, have focused too narrowly upon particular issues to provide any cohesiveness for a set of uniform informational privacy laws in the United States. For instance, in California, credit card companies are required to notify the consumer about the privacy policy and, furthermore, the consumers are given an option to opt-out.[74] This is similar to a Virginia statute that prohibits, in certain limited circumstances, the information gathered "solely as the result of any customer payment . . . by credit card" unless the merchant gives notice to the consumer.[75] Along the same vein, a number of states have enacted "Do Not Call" lists that ban telemarketers.[76] Some states have also turned their attention to spam e-mail messages. For example, Tennessee requires subject headings to be designated with "ADV," or an advertising label.[77] These diverse measures, however, exemplify the discontinuity of informational privacy laws enacted by states; instead of providing citizens with blanket legislation that provides protection of data collection practices, states focused on singular practices.

B. Proposed Bill: Stronger Federal Regulations, But Lack of Consistent Standards

In an attempt to provide cohesive data collection laws that protect informational privacy, federal legislators have proposed legislation that would provide blanket regulation of data collection. It should be noted that federal legislation is beneficial because it can provide clear standards, align with consumer behaviors, and allow for amendments more quickly than case law.[78] In May 2010, Representatives Rich

72. Defendant Response to Plaintiff's Motion to Stay Pending Petition for Writ of Certiorari, Boring v. Google, Inc., 598 F. Supp. 2d 695 (W.D. Pa. 2009) (No. 08-cv-694), *available at* http://www.zegarelli.com/Cases/Borings%20v%20Google/Google%20Response%20to%20Motion%20web.pdf (consent judgment).

73. *See* Sovern, *supra* note 47, at 1312–15. *See, e.g.,* VA. CODE ANN. § 59.1-442 (1998), CAL. CIV. CODE § 1748.12(b) (West 1998).

74. CAL. CIV. CODE § 1748.12(b) (West 1998); *see* Sovern, *supra* note 47, at 1315.

75. Sovern, *supra* note 47, at 1315; VA. CODE ANN. § 59.1-442 (1998).

76. Sovern, *supra* note 47, at 1315. *See, e.g.*, ALASKA STAT. ANN. § 45.50.475 (West 2006).

77. TENN. CODE ANN. § 47-18-2501(e) (Supp. 2000); Sovern, *supra* note 47, at 1317.

78. *See, e.g.*, Sovern, *supra* note 47, at 1312–13.

Boucher and Cliff Stearns, members of the House of Representatives Subcommittee on Communications, Technology and the Internet, introduced a draft bill that proposed new Internet privacy regulations.[79] The unnamed bill was met with criticism from both Democrats and Republicans in Congress.

The proposed bill expanded the definition of sensitive information to include an individual's Internet Protocol (I.P.) address, name, race or ethnicity, precise location, or any user-entered preference profile.[80] Hence, if any of this personal information could be used to identify a user, companies would be required to provide users with notice.[81] The proposal would require companies to include descriptions of how the information is collected, stored, and the duration of the data storage.[82]

The issues of consent and opt-out were heavily disputed in the 2010 draft bill. Under the proposal, an individual is deemed to have consented to the collection of data by either affirmatively granting consent or failing to decline consent at the time a clear statement is conveyed to the individual.[83] Thus, the proposal allowed for implied consent. Privacy advocates like Jeffrey Chester, the Director for the Center for Digital Democracy, were disappointed that the proposal relied upon consent.[84] Chester said, "The flaw is that it forces consumers to rely on digital fine print. It's still buried in the privacy policies."[85]

While this requirement applied to marketers and advertisers, the bill made exceptions for entities that delete information within eighteen months.[86] Nevertheless, advertisers and marketers found the notice requirement too restrictive.[87] They argued that behavior advertising allows everyone to benefit from free Internet service.[88] If consent notices were required, then costs would be imposed upon Internet

79. Discussion Draft, *supra* note 21.

80. *Id.* §§ 2(5), 2(6), 2(8)–2(11).

81. *Id.* § 3(a).

82. *Id.* § 3(a)(2)(B).

83. *Id.* § 3(a)(3)(A)(ii).

84. *See* Stephanie Clifford, *Privacy Bill Finally in Draft, as Both Sides Weigh In*, MEDIA DECODER BLOG (May 4, 2010, 2:14 PM), http://mediadecoder.blogs.nytimes.com/2010/05/04/privacy-bill-finally-in-draft-as-both-sides-weigh-in/.

85. *Id.*

86. Discussion Draft, *supra* note 21, § 3(e)(2).

87. Clifford, *supra* note 84.

88. Letter from Daniel Castro, Senior Analyst, The Information Technology & Innovation Foundation, to Rick Boucher, Congressman, and, Cliff Stearns, Congressman, Subcomm. on Commc'ns, Tech. & the Internet, (May 25, 2010) [hereinafter ITIF Letter], *available at* http://www.itif.org/files/2010-privacy-legislation-comments.pdf.

service providers who would in turn pass this cost on to the consumer.[89] However, in a *New York Times* interview, Congressman Boucher disagreed with the assessment that this proposed provision would hinder businesses. He instead noted: "Our goal is to enhance electronic commerce - we are not seeking in any way to disable targeted advertising."[90]

The proposed bill would delegate more authority to the FTC to implement and enforce informational privacy rights. The Commission would be responsible for the enforcement of the act[91] and it would have the authority to amend or enact regulations to carry out the act.[92] Alternatively, because the proposed bill does not allow for a private right of action, the state attorney general could bring a claim on behalf of a citizen of the state.[93] The Commission would still retain the authority to intervene, however.[94] Moreover, if the FTC pursued a civil action against a defendant, the state attorney general would be prohibited from bringing a lawsuit.[95]

The proposed Internet privacy bill also preempted state privacy laws.[96] This provision was met with approval by the Information Technology & Innovative Foundation (ITIF), a non-partisan public policy think tank committed to advancing a pro-technology public policy agenda.[97] In a letter to the Congressmen Boucher and Stearns, ITIF noted that a federal framework that established a single standard of law would make it easier for the private sector to meet compliance.[98]

As Congress opened its 112th session in 2011, the issue of Internet privacy was gaining traction. This was due in part to President Obama's November 2010 announcement that he planned to appoint a "privacy czar" to oversee the implementation of new privacy laws.[99] The Obama administration took a more hands-on approach to Internet regulations compared to previous administrations because of the central role of personal information.[100] Moreover, new congressional representatives,

89. *Id.*
90. Clifford, *supra* note 84.
91. Discussion Draft, *supra* note 21, § 8(a).
92. *Id.*
93. *Id.* § 8(b).
94. *Id.* § 8(b)(2).
95. *Id.* § 8(b)(2)(B).
96. *Id.* § 10.
97. ITIF Letter, *supra* note 88, at 2.
98. *See generally id.*
99. Julia Angwin, *Watchdog Planned for Online Privacy*, WALL ST. J. (Nov. 11 2010), http://online.wsj.com/article/SB10001424052748703848204575608970171176014.html.
100. *Id.*

who were likely to have a strong influence on Internet and data collection legislation, also expressed interest in the issue. In February 2011, Jackie Speier, a congresswoman from California, introduced the "Do Not Track Me Online Act."[101] This bill would give the FTC the powers to create a national opt-out option for Internet users and to impose financial penalties for violations of the act.[102] This "Do Not Track" mechanism is similar to one suggested by the FTC, which noted in December 2010:

> One way to facilitate consumer choice is to provide it in a uniform and comprehensive way . . . The most practical method of providing such universal choice would likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signaling the consumer's choices about being tracked and receiving targeted ads. Commission staff supports this approach, sometimes referred to as a 'Do Not Track.'[103]

Thus, with such an emphasis on privacy issues, the 2010 draft bill was likely to be rewritten by the 112th Congress.

Furthermore, any revisions of the 2010 draft bill would likely take into account a December 2010 report dealing with online privacy written by the Department of Commerce Internet policy task force.[104] After a year-long review, the eighty-eight page report called for Internet businesses to develop a bill of rights to protect consumer data privacy.[105] The report also called for the Obama administration to form a new government office to oversee these privacy efforts.[106] The Commerce Department, however, did not call for comprehensive privacy legislation. Rather, the report suggested that companies voluntarily

---

101. *See generally* Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011) [hereinafter H.R. 654], *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr654ih/pdf/BILLS-112hr654ih.pdf.

102. *See* H.R. 654 §§ 3, 5.

103. FED. TRADE COMM'N, PRELIMINARY STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE - A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS vi–vii (2010) [hereinafter FTC PRELIMINARY STAFF REPORT], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

104. *See generally Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, U.S. DEPARTMENT COM. (Dec. 16, 2010) http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf [hereinafter *Commercial Data Privacy*] (for the full report).

105. *Commerce Department Unveils Policy Framework for Protecting Consumer Privacy Online While Supporting Innovation*, U.S. DEPARTMENT COM. (Dec. 16, 2010), http://www.commerce.gov/news/press-releases/2010/12/16/commerce-department-unveils-policy-framework-protecting-consumer-priv [hereinafter *Consumer Privacy Press Release*].

106. *See Commercial Data Privacy*, *supra* note 104, at 44; *see also Consumer Privacy Press Release*, *supra* note 105.

agree to comply with principles that protect consumer information.[107] Companies that complied with the voluntary code of conduct could receive safe harbor protection.[108] Thus, the safe harbor would create broad protection for entities that demonstrated compliance with the code by providing those entities with certain immunities.[109] Nonetheless, Secretary of Commerce Locke conceded that stronger enforcement is necessary for this self-regulation to work.[110]

In 1973, the Department of Health, Education, and Welfare outlined a Code of Fair Information Practices (FIPPs)[111] that would create "safeguard requirements" for certain "automated personal data systems" maintained by the Federal Government.[112] The Commerce Department suggested that adoption of baseline FIPPs, akin to a "Privacy Bill of Rights," would outline "a clear set of principles" that could guide "how companies collect and use personal information for commercial purposes."[113] The task force concluded that the proposed bill of rights would close gaps in the current policy, provide greater transparency, and increase certainty for businesses to reach compliance.[114] The Commerce Department noted that an important concern of any regulation is its impact on the business sector.[115] In fact, the FIPPs were designed to encourage innovation by businesses—a key factor in whether any privacy bill received Republican support.[116] Thus, it was not surprising when Senators John McCain and John Kerry introduced yet another privacy bill that placed a three million dollar penalty cap for privacy violations.[117]

Nevertheless, privacy advocacy groups argued that this accommodation of the business sector was not enough to protect Internet users and, moreover, was likely to only result in maintenance of the status quo. Jeff Chester, founder of the Center for Digital

107. *See Commercial Data Privacy*, *supra* note 104, at 41.

108. *Id.*

109. *Id.* at 44.

110. Jim Puzzanghera, *U.S. Proposes Online Privacy Bill of Rights*, L.A. TIMES (Dec. 16, 2010), http://articles.latimes.com/2010/dec/16/business/la-fi-obama-privacy-20101217.

111. Commonly referred to as *Fair Information Practice Principles* (FIPPs).

112. U.S. DEP'T OF HEALTH, EDUC., & WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS § 4 (1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm; *see also Commercial Data Privacy*, *supra* note 104, at 11.

113. *Consumer Privacy Press Release*, *supra* note 105; *see Commercial Data Privacy, supra* note 104, at vii, 3–5, 11, 23–24, 70; Puzzanghera, *supra* note 110.

114. *Commercial Data Privacy*, *supra* note 104, at vii.

115. *See id.*

116. *Id.*

117. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011) § 404(c).

Democracy, noted that the proposed "framework is based on industry self-regulation."[118] Privacy advocates, however, desire stronger government regulation. As Susan Grant, director of consumer protection for the Consumer Federation of America said: "It's good that the Department of Commerce recognized we have a privacy problem, but the solution isn't more self-regulation. We've tried that and it's clearly inadequate. We need a privacy law that sets the rules of the road."[119]

III. BACKGROUND OF E.U. LAW

In contrast to the United States, privacy law in Europe has developed as a personal dignity rather than a liberty.[120] The notion of privacy as a dignity is suggested by Article 8 of the European Convention on Human Rights, which protects the "right to respect for private and family life."[121] Furthermore, the European Union's new Charter of Fundamental Rights protects both "respect for private and family life" and "protection of personal data."[122] In another example of the importance Europeans place upon informational privacy, the German state of Hesse drafted the world's first data-protection law in 1970.[123] These examples illustrate that the European Union has taken a more regulatory role in informational privacy than the United States.[124]

A. European Union: Umbrella Legislative Model That Provides a Uniform Approach to Data Collection Privacy Laws

Europe has achieved legal uniformity for data collection through its directives.[125] European Union directives are legislative acts that require member states to achieve a desired result.[126] In turn, member

118. Angwin, *supra* note 99; *see also* Puzzanghera, *supra* note 110.

119. Puzzanghera, *supra* note 110.

120. *See generally* Whitman, *supra* note 37 (discussing different notions of privacy across European and American society).

121. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, para. 1, 213 U.N.T.S. 221, 230.

122. Charter of Fundamental Human Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) 10.

123. Hessisches Datenschutzgesetz [HDSG] [Hessian Data Protection Act], *Hess* GVBl. I. 625 (1970).

124. *See also* Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 UNIV. OTTAWA L. & TECH. J. 357, 361 (2005), *available at* www.uoltj.ca/articles/vol2.2/2005.2.2.uoltj.Levin.357-395.pdf (comparing restrictions placed by the US and EU governments on private sector use of personal information).

125. *Id.*

126. *Application of EU Law,* EUR. COMMISSION (June 11, 2012), http://ec.europa.eu/eu_law/directives/directives_en.htm.

states must then adopt legislation that complies with the directives.[127] The Data Protection Directive 95/46/EC gave member states until 1998 to implement data collection legislation. The directive broadly defined personal data as "any information relating to an identified or identifiable natural person . . . who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physiological, mental, economic, cultural or social identity."[128] Member states were required to create a supervisory authority to monitor the state's compliance with the directive.[129] The supervisory authority has investigative powers as well as the power to engage in legal proceedings.[130] The directive also allows for individuals to object to the processing of personal data for direct marketing purposes.[131] Additionally, individual citizens can bring complaints of violations to the supervisory authority or the court, and are entitled to relief as a result of the unlawful processing of their personal data.[132]

B. United Kingdom: Europe's Least Stringent Data Collection Laws

In 1998, the United Kingdom passed the Data Protection Act, which met the requirements of the EU directive.[133] Although the UK laws met the requirements at the time of promulgation, UK data collection legislation is among Europe's most relaxed. Consent, for example, is often deemed implied for non-sensitive data.[134] Consent for sensitive data can take many forms, including written, oral, or by the clicking of a box.[135] This is in contrast to Germany's laws, which call for consent to be in writing.[136]

In 2009, it was reported that the United Kingdom failed to properly implement eleven of the directive's thirty-four articles, or nearly a third of the directive.[137] Later that year the EU Telecoms Commission opened

127. *Id.*
128. *Council Directive 95/46*, *supra* note 32, art. 2.
129. *Id.* art. 17.
130. *Id.* art. 28.
131. *Id.* art. 14.
132. *Id.* art. 22.
133. Data Protection Act, 1998, c. 29 (Eng.).
134. *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments: Final Report*, at 31 (Jan. 20, 2010) [hereinafter Commission Comparative Study Final Report], *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.
135. A.6—United Kingdom, *supra* note 34, at 29.
136. A.4—Germany, *supra* note 33, at 17.
137. A.6—United Kingdom, *supra* note 34, at 1.

an infringement proceeding against the United Kingdom.[138] The Commission found that behavioral advertising, which monitors users' Internet interests and then delivers targeted advertisements, was not properly regulated.[139] In that instance, users were not properly informed of the data collection.[140] Furthermore, the Telecoms Commission found that the United Kingdom lacked an independent national supervisory authority to oversee regulations.[141] This incident highlighted aspects of the disharmony within the European Union: namely, compliance and enforcement of the directive by the member states.[142]

A European Commission report highlighted the narrow approach that the United Kingdom has taken with regard to personal data.[143] The Court of Appeal case *Durant v. Financial Services Authority* narrowed the definition of what constitutes personal data.[144] There, the court found that personal data did not extend to information focusing on things other than the individual.[145] Additionally, the United Kingdom made nuanced distinctions of when IP addresses constitute personal data. Rather than provide a bright-line rule, UK authorities have defined IP addresses as either "dynamic" or "static."[146] Static IP addresses are classified as personal data because they retain information regarding a particular individual.[147] On the other hand, dynamic IP addresses contain information regarding a particular computer but are not linked to an individual user. Consequently, dynamic IP addresses do not fall within the definition of personal data.[148] The EU report found that the UK approach deviates from that of other EU countries.[149]

The Information Commissioner's Office (ICO) carries out enforcement of data protection in the United Kingdom.[150] The UK government sponsors the ICO, raising doubts about whether this structure complies with the directive statute that ensures that the

138. Press Release, European Union, Telecoms: Commission Launches Case Against UK Over Privacy and Personal Data Protection (Apr. 14, 2009), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en.

139. *Id.*

140. *Id.*

141. *Id.*

142. *See* Commission Comparative Study Final Report, *supra* note 134, ¶ 17.

143. A.6—United Kingdom, *supra* note 34, at 1.

144. Durant v. Financial Services Authority, [2003] EWCA (Civ) 1746, ¶ 28 (Eng.).

145. *Id.; see* A.6—United Kingdom, *supra* note 34, at 5.

146. A.6—United Kingdom, *supra* note 34, at 6.

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id.* at 59.

supervisory authority acts with complete independence.[151] The ICO commissioner lacks the power that other European states give to the supervisory authority. For instance, the ICO commissioner does not have autonomous power to demand access to data.[152] Rather, the commissioner must first apply for a search warrant from a judge.[153] In 2006, the ICO applied for only seven such warrants.[154]

Recently, however, the ICO commissioner has been granted more powers.[155] The commissioner can now impose a monetary penalty.[156] Further, the ICO can now audit an organization's data processing practices without the organization's consent.[157] Despite these new powers, the EU report expressed doubts that these measures would lead to stronger enforcement, in part, because the ICO has been reluctant to exercise its already-existing power.[158] The report pointed specifically to the fact that the ICO generally investigates instances that are first exposed by the media.[159] Moreover, most of the cases that had been brought to the attention of the ICO were simply dealt with by giving advice and guidance.[160] Thus, the EU report concluded, these additional powers would likely only be exercised in the most egregious and easiest to prove data security breaches.[161]

C. Germany: Europe's Strictest Data Collection Laws

Data collection regulations in Germany have a strong constitutional basis.[162] After the region of Hesse adopted the world's first data protection law in 1970, the first German federal law was passed seven years later. The subsequent development of these laws was reflected in the 1983 German Constitutional Court's finding of a fundamental right to "informational self-determination" in the German constitution.[163] Consequently, under the German constitution, an individual has the right to determine for himself the disclosure or use of

151. *Id.*
152. A.6—United Kingdom, *supra* note 34, at 60.
153. *Id.*
154. *Id.*
155. Criminal Justice and Information Act, 2008, c. 4, § 144.
156. *Id.*
157. A.6—United Kingdom, *supra* note 34, at 61.
158. *Id.* at 62.
159. *Id.*
160. *Id.*
161. *Id.* at 73.
162. A.4—Germany, *supra* note 33, at 1.
163. *Id.* at 2.

his personal information.[164] Germany has continued to adopt strong privacy laws that protect the collection of informational data.[165] Most scholars agree that the German stance on privacy is the result of the country's history of Nazism.[166] Today, there are sixteen general data protection laws in Germany and many other laws dealing with data protection in specific contexts or that otherwise bear on data protection.[167] Thus, the result is a collection of data protection laws that is both detailed and technical.

The German high court expressed its wariness of overreaching EU law when it approved the Treaty of Lisbon. There, the Constitutional Court stated in its June 2009 decision:

> If legal protection cannot be obtained at the Union level, the Federal Constitutional Court examines whether legal instruments of the European institutions and bodies keep within the boundaries of the sovereign powers accorded to them by way of conferral . . . [T]he fundamental political and constitutional structures of sovereign Member States . . . cannot be safeguarded in any other way.[168]

Hence, the German Constitutional Court has retained the ultimate right to test the validity of European law under the German Constitution.[169] The issue of data collection is an area where the question of supremacy of constitutional or European law is likely to be raised. Because of the German Constitutional Court's previous rulings, such a situation would result in the Court regarding any European rules that fall short of the Court's standards as "invalid and unenforceable."[170]

In Germany, data protection often rests on complex "balance" provisions.[171] The EC report noted, however, that this test is too vague.[172] In several circumstances within the private sector, data processing for secondary purposes is allowed without consent.[173] In these contexts, a balancing test is used that favors the private sector.[174]

---

164. *Id.*
165. *Id.*
166. Whitman, *supra* note 37, at 1180.
167. A.4—Germany, *supra* note 33, at 3.
168. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] June 30, 2009, Entscheidungen des Bundesverfassungsgerichts [BVerfGE], ¶ 240 (Ger.).
169. A.4—Germany, *supra* note 33, at 1.
170. *Id.*
171. *See* Federal Data Protection Act, *supra* note 3, §§ 28(1), 29(1), 30(2).
172. A.4—Germany, *supra* note 33, at 12.
173. *See id.* at 20 (processing of personal data in the private sector on the basis of statutory authorization).
174. *Id.*

This test, however, is also employed for the public sector.[175] It is necessary to note that the EU Data Protection Directive allows for processing when it is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority."[176] Germany, however, has included stricter protection than the directive requires by implementing provisions that limit data collected specifically by the body carrying out the task.[177] When the balance test is employed in these instances, the balance is "tilted against the public sector."[178]

Nevertheless, the enforcement system in Germany is not as strong as might be expected. In the public sector, the role of the federal and state data protection commissioners is limited.[179] For example, the federal commissioner can demand a formal review but cannot order specific changes.[180] Thus, the commissioner's role is not one of significant legal power. Conversely, in the private sector, supervisory authorities are granted extensive powers of investigation and enforcement.[181] The supervisory authority can demand "any information which the supervisory authority needs for the fulfillment of its task,"[182] and the information must be provided without delay.[183] Moreover, the authority can carry out inspections of documents and personal data files.[184] With regard to enforcement, the supervisory authority can set a deadline for the compliance of certain measures and impose administrative fines.[185]

In 2009, Germany enacted additional amendments to the Federal Data Protection Act. These amendments required notification of data security breaches and strengthened regulation of data marketers.[186] Additionally, the amendments increased fines from €25,000 to €50,000 for violations of the law.[187] These changes also strengthened the power of the data protection authorities. For example, when a data controller

175. *Id.* at 19.
176. Council Directive 95/46, *supra* note 32, art. 7(e).
177. *See* Federal Data Protection Act, *supra* note 3, § 13.
178. A.4—Germany, *supra* note 33, at 19.
179. *Id.* at 52.
180. *Id.*; *see* Federal Data Protection Act, *supra* note 3, § 25.
181. A.4—Germany, *supra* note 33, at 52; *see* Federal Data Protection Act, *supra* note 3, § 38.
182. A.4—Germany, *supra* note 33, at 52.
183. Federal Data Protection Act, *supra* note 3, § 38.
184. *Id.* §§ 24, 38(4).
185. A.4—Germany, *supra* note 33, at 53; *see* Federal Data Protection Act, *supra* note 3, § 38(5).
186. Federal Data Protection Act, *supra* note 3, § 33.
187. *Id.* § 43(3).

notifies the supervisory authority about a breach, an investigation will be launched followed by stiffer fines.[188]

Nonetheless, it is necessary to consider the context of a modern technological society in which EU data collection laws operate. Germany, for instance, had a population of over 81 million in 2010.[189] All versions of the iPhone sold out within days.[190] There were an estimated 7.7 million German Facebook users as of May 2010.[191] Although Germany was the only country to offer an opt-out option for Google's Street View service before its launch, only an estimated 250,000 people, or three percent of the population, exercised this option.[192] In fact, some Germans embraced the Street View mapping, with the mayor and tourist board of Oberstaufen, Germany inviting Google to put their town on the map and even baking a cake for the occasion.[193]

The United Kingdom, with less stringent data collection laws, has experienced much of the same consumer behavior. As of March 2011, for instance, there were 30 million Facebook users in the United Kingdom, which has a population of about 63 million.[194] Thus, consumer behavior in both the United Kingdom and Germany illustrate a growing disconnect with Germany's strict data collection laws.

IV. COMPARATIVE ANALYSIS OF U.S. AND E.U. DATA COLLECTION PRIVACY LAWS

A. The Proposed United States Internet Bill is the Functional Equivalent of an EU Directive, But Would Eliminate the Disharmony Within EU Laws

By analyzing the EU approach to data collection privacy laws, the United States can gain valuable insight. The EU's blanket legislation provides member states with uniform standards. This system is not infallible, however. In fact, there is much disharmony of data protection

188. *Id.* §§ 42a, 43.

189. *The World Factbook: Germany*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/gm.html (last visited Aug. 10, 2012).

190. O'Brien, *supra* note 8.

191. *Id.*

192. *German Street View Goes Live with Enhanced Privacy*, BBC NEWS (Nov. 2, 2010), http://www.bbc.co.uk/news/technology-11673117.

193. *Id.*

194. Daily Mail Reporter, *Network Nation: Facebook Users in the UK Surges to Half of the Population*, DAILY MAIL (Mar. 7, 2011), http://www.dailymail.co.uk/news/article-1362413/Facebook-users-UK-surges-HALF-population.html#.

laws within the EU. Thus, the United States should be mindful of the strengths and limitations of the E.U. system when adopting new data collection privacy laws.

The proposed May 2010 U.S. Internet privacy bill provides a blanket federal law that serves as the functional equivalent of an E.U. directive.[195] Thus, the promulgation of a federal law would provide states with a uniform standard. While the EU has implemented uniform standards, there has been disharmony with the variation and enforcement of these standards. It should be noted, however, that the proposed U.S. bill includes a preemption clause, allowing the law to supersede conflicting state regulations. This move toward national uniformity could avoid the disharmony the EU experiences with regulation and enforcement of data protection laws.[196]

1. Disharmony Within EU Law: Variations of Standards

Although EU Member States enact legislation with similar wording, application of these laws varies significantly, often resulting in disharmony.[197] This is in part because countries apply different tests, ranging from "reasonable expectations," "fairness," or even "balancing" tests.[198] Another divergence occurs when countries delineate exceptions for the public sector. UK law, for instance, makes exceptions for broadly defined "policing purposes."[199] On the other hand, Germany provides exceptions for more tailored instances that include "countering immediate threats," "general and specific prevention," and "investigation and prosecution of [suspected] criminal offences."[200] Moreover, these differences are further exacerbated when the adjudication of multi-national issues is necessary.[201]

2. Disharmony Within EU Law: Enforcement of Standards

One shortcoming of EU law was addressed in a March 2010 opinion paper that examined the principle of accountability and enforcement of data collection rights in Europe.[202] The Article 29

195. Discussion Draft, *supra* note 21.
196. *Id.* § 10.
197. Commission Comparative Study Final Report, *supra* note 134, ¶ 50.
198. *Id.*
199. *Id.*
200. *Id.*
201. *Id.*
202. *Opinion 3/2010 on the Principle of Accountability*, Article 29 Data Protection Working Party, 00062/10/EN WP 173 (July 13, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

Working Party that was responsible for this opinion was concerned about whether the implementation of data protection requirements resulted in effective mechanisms, and, in turn, delivered real protection to Internet users.[203] As the opinion paper noted, the Article 29 Working Party wanted to move from "theory to practice."[204] With this in mind, the paper advanced a proposal for accountability that would require data controllers to put in place appropriate and effective measures to ensure compliance with the principles and obligations set forth in the directive and to further demonstrate such compliance to the member state's supervisory authorities.[205]

While the new proposal does not introduce any requirements that do not already exist under current law, it does set forth provisions that ensure compliance. For instance, Directive 2002/58 was amended in 2009 and called for "the implementation of a security policy with respect to the processing of personal data."[206] The Working Party report is evidence of the need for clear legal standards ensuring Member States meet both the standards and implementation requirements of the data protection directives.[207]

3. The Need for a Preemption Clause

The disharmony within the EU is an excellent example of the need for clear, cohesive laws. A blanket federal law in the United States would create a clear standard with which states can comply. With the inclusion of a preemption clause, this umbrella legislation could help the United States avoid some of the disharmony EU countries face. Such a clause would preempt state privacy laws. Although some states have given citizens more privacy rights through legislation, these laws have been narrowly tailored to combat a single problem like spam e-mail messages or telemarketers.[208] Thus, states have not provided comprehensive data protection legislation. Nevertheless, a blanket data collection law with a preemption clause would provide a clear standard for all fifty states.

The Commerce Department's 2010 report called for a narrowly tailored preemption clause.[209] Citing concerns of businesses, the report

203. *Id.* ¶ 1.
204. *Id.*
205. *Id.* ¶ 74.
206. *Id.* ¶ 37.
207. *Id.* ¶ 74.
208. *See, e.g.*, WASH. REV. CODE § 19.190.030 (regarding unpermitted or misleading electronic email).
209. *Commercial Data Privacy*, supra note 104, at 62.

suggested that states could provide remedies more quickly and take into consideration developing technologies when enacting legislation.[210] One proposal was to limit preemption to state laws that addressed the same subject matter.[211] Another suggestion called for the state attorneys general to enforce federal law while preserving state laws.[212]

Compliance is only one aspect of the problems the EU faces. Enforcement of data protection laws has proven to be another challenge.[213] Under the current U.S. system, the FTC holds regulatory power but only regulates for "unfairness" and "deception" practices.[214] Thus, any effective data collection legislation will require a regulating authority with more power. This could be accomplished by either granting the FTC more regulatory authority or by creating a separate commission with more authority. It should be noted that all the recent legislative bills that have been introduced have proposed granting the FTC more regulatory authority.[215]

In its task force report, the Commerce Department suggested that the FTC remain the primary enforcement agency.[216] The report called for the creation of an authority to convene business and civil society groups to develop effective, consensus-based voluntary codes.[217] The proposed authority, called the Privacy Policy Office (PPO), would work alongside the FTC, but it would have no enforcement authority of its own.[218] Instead, the PPO would serve as a center of commercial data privacy policy expertise.[219] The office would also help foster policy that takes into consideration the potential effects on both businesses and consumers. For instance, the PPO would suggest where new industry privacy codes are needed based on consumer complaints, research, and industry initiatives.[220] The creation of the PPO demonstrates the Commerce Department's recognition of the need for stronger

210. *Id.* at 61.
211. *Id*. at 62.
212. *Id.*
213. *See* Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 CHI. J. INT'L L. 233, 234–35 (2007).
214. Chris Hoofnagle, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments: B.1—United States of America*, EUR. COMM'N 18–19 (May 2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf [hereinafter *B.1—United States of America*].
215. *See, e.g.*, Discussion Draft, *supra* note 21, § 8(b)(2); H.R. 654, *supra* note 102, §4.
216. *Commercial Data Privacy*, *supra* note 104, at 51.
217. *Id.* at 44.
218. *Id.* at 45–46.
219. *Id.* at 45.
220. *Id.* at 48.

regulations. It further illustrates that privacy policies must be enforced by a single, powerful entity if effective data collection laws are to be accomplished.

B. Effective Legislation: The Delineation of Consistent Consent and Opt-Out Policies

For the successful implementation of effective data protection legislation, the United States will have to delineate consistent consent and opt-out policies. The varying levels of consent within the United States' current laws demonstrate the uneven landscape of data protection.[221] In fact, an EU study noted that inconsistent levels of consent in U.S. law resulted in large gaps within privacy laws.[222] This problem is not exclusive to the United States, however. The EU has also encountered similar problems. This is exemplified by the disparity between laws in the UK and Germany. For example, consent is often deemed implied in the UK.[223] Germany, however, stipulates that consent is "only valid if it is based on the free decision of the person concerned."[224] Thus, to create cohesive legislation, the United States will have to adopt clearly defined policies.

Any proposal of new data collection laws will surely meet resistance from the business sector. In January 2011, it was reported that Facebook changed its lobbying status in Washington, D.C. because stronger privacy legislation was being debated.[225] Current laws allow businesses to use personal information without consent and without giving individuals the opportunity to opt-out.[226] Furthermore, companies are allowed to vaguely state their privacy policies.[227] These practices have occurred largely because the business sector is allowed substantial latitude. As the Commerce Department's report cites, the commercial

---

221. *See, e.g.*, *id.* at 2 (majority consensus that there is a need for a "baseline commercial data privacy framework").

222. *See, e.g.*, *B.1—United States of America*, *supra* note 214, at 4 (noting that in the surveillance context, federal law requires "one-party consent" while states follow an "all-party consent" model for recording conversations).

223. Press Release, European Union, Telecom: Commission Launches Case Against UK over Privacy and Personal Data Protection (Apr. 14, 2009) *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en.

224. A.4—Germany, *supra* note 33, at 7.

225. Jon Swartz, *Facebook Changes Its Lobbying Status in Washington*, USA TODAY (Jan. 12, 2011), http://www.usatoday.com/money/industries/technology/2011-01-13-facebook13_CV_N.htm.

226. *See B.1—United States of America*, *supra* note 214, at 41.

227. *Id.* at 28.

sector is given deference because the government does not want to stifle innovation.[228] Thus, with such an emphasis placed on economic considerations, the United States may not be able to adopt EU-like data protection laws.[229]

C. Effective Legislation: The Implementation of Remedial Measures for Individuals

The proposed U.S. bill does not provide a right of action for individuals.[230] Although this approach is similar to that of the EU, a recent EU report called for improving this provision. In the report, the Commission advocated for individual rights and remedies that were effective, speedy, and cheap.[231] The report further noted the need for specific remedial rights to be outlined in any upcoming amendments.[232] To improve the situation in the EU, the report also called for non-governmental and civil groups to be granted standing so they can bring actions on behalf of individuals.[233] Moreover, the report noted that class action lawsuits in the United States should serve as a model for how the EU legal system could better provide individuals with remedies for their grievances.[234]

Finally, another issue addressed by the Commission was damages. The Commission urged liquidated damages to be higher than the cost of non-compliance.[235] This would incentivize entities to comply with the directions in the law. These recommendations underscore the shortcomings of remedies that are currently available to individuals in the EU system. Therefore, before doing away with an individual's redress, U.S. legislators should consider the implications of such measures.

---

228. *See Commercial Data Privacy*, *supra* note 104, at iii.

229. In January 2012, the EU Commission proposed comprehensive reform to data protection rules that called for a Regulation to be immediately binding on Member States. Thus, the Regulation would avoid the varying levels of interpretation of the Directive by each Member State, which has consequently led to disharmony within the EU. *See* European Commission, *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 Movement of Such Data*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

230. Discussion Draft, *supra* note 21, § 9.

231. Commission Comparative Study Final Report, *supra* note 134, ¶¶ 110–11.

232. *Id.*

233. *Id.* ¶ 111.

234. *Id.*

235. *Id.* ¶ 112.

V. CONCLUSION

In any comparative analysis of privacy laws, it is necessary to note that European and American notions of privacy differ. Furthermore, while scholars have debated the origin of American notions of privacy, such an origin is unlikely to be monocausal.[236] Thus, a fierce protection of the home, a distrust of the government, or a misunderstanding of the commercial sector's privacy protection practices is unlikely to be the singular source of American notions of privacy.[237]

European privacy has developed as a "personal dignity," whereas privacy within the United States has developed as a "liberty."[238] Privacy laws within the United States have protected individuals from intrusions by the State and have provided protection for decisional privacy.[239] Informational privacy, however, has not received such protection and is regulated by a patchwork system of federal and state laws.[240] The result is a system that lacks consistent and cohesive standards.

An incident with the social networking site Facebook illustrates the notion that consumers' desire more protection for their personal information. Facebook experienced widespread user revolt when users became aware of the website's new news feed, its "Beacon" service, and changes in the terms of its service policy.[241] The "Beacon" service allowed a user's Facebook "friends" to track the user's "purchases on partner websites,"[242] and the "news feed" feature allowed "friends" to track a user's use of the website.[243] The changes in the company's terms of service gave Facebook a "perpetual license for user-submitted content," even after an account was terminated.[244] While these policies were not unusual for Internet companies in the United States,[245] Facebook users expressed their discomfort with the company's

236. Kumayama, *supra* note 31, at 429–30.

237. *See* Whitman, *supra* note 37, at 1161 (arguing that respect and personal dignity are at the core of U.S. notions of privacy).

238. *Id.*

239. *Id.*

240. *Id.* at 1193.

241. *B.1—United States of America, supra* note 214, at 6.

211. Partner websites are websites chosen by Facebook, which are given user data in order to give individuals "a more personalized experience." *See Facebook Help Center – Instant Personalization*, FACEBOOK, http://www.facebook.com/help/?page=202975766411357 (last visited Aug. 12, 2012).

243. *B.1–United States of America*, *supra* note 214, at 6.

244. *Id.* As of April 26, 2011, the Facebook terms state the "IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it." Statement of Rights and Responsibilities, FACEBOOK (June 8, 2012), http://www.facebook.com/terms.php?ref=pf.

245. *Id.*

policies.[246] This example suggests that "Americans would object to many common business uses of personal information."[247]

Similarly, Apple received criticism in April 2011, when it was reported that its iPhones and iPads recorded and collected user location data.[248] The revelation caused an outcry from users and privacy watchdogs alike.[249] Apple responded by providing a software update and releasing a statement noting that it was not tracking the location of users' iPhones, but merely collecting information to improve its location and traffic information databases.[250] The episode highlighted the fact that while users are willing to share this information as part of a service, this information is deemed sensitive enough that users do not want the information recorded.[251] Thus, the Facebook and Apple examples further indicate the balance that must be struck with privacy in a digital age.

As the United States adopts new data collection laws, it may look to the EU as a model. Although the EU provides cohesive data collection laws, its system is not infallible. When analyzing the UK and Germany, a disparity of standards between the countries is evident. Germany has some of the strictest data collection laws in the world, while the UK has some of the least stringent. Moreover, enforcement of EU directives is, at times, uneven. Lastly, the EU system places

246. Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES (Nov. 30, 2007), http://www.nytimes.com/2007/11/30/technology/30face.html.

247. *B.1–United States of America*, *supra* note 214, at 6.

248. *Apple Pressed in iPhone, iPad Tracking Furor*, CBSNEWS.COM (Apr. 21, 2011), http://www.cbsnews.com/stories/2011/04/21/scitech/main20056206.shtml.

249. *Id.; see also Apple Sued over iPad and iPhone Location Tracking Issue*, PADGADGET (Apr. 25, 2011), http://www.padgadget.com/2011/04/25/apple-sued-over-ipad-and-iphone-location-tracking.

250. *Apple Q&A on Location Data*, APPLE (Apr. 27, 2010), http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html*; Internet Data Collection: The Privacy Line*, L.A. TIMES (May 8, 2011), http://articles.latimes.com/2011/may/08/opinion/la-ed-privacy-20110508 [hereinafter *The Privacy Line*]; *see also* MARY MADDEN & AARON SMITH, REPUTATION AND SOCIAL MEDIA: HOW PEOPLE MONITOR THEIR IDENTITY AND SEARCH FOR OTHERS ONLINE 29 (2010), http://pewinternet.org/Reports/2010/Reputation-Management.aspx (noting that 71 percent of social networking users ages 18–29 have changed profile privacy settings limiting information shared online).

251. *The Privacy Line*, *supra* note 250; *see also* Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, 6 J.L. & POL'Y INFO. SOC'Y 119, 119 (2010). Tsai et al. conducted an online survey of 587 of American Internet users "to evaluate users' perceptions of the likelihood of several location-sharing use scenarios along with magnitude of the benefit or harm of each scenario." Tsai et al., *supra*. Based on the survey, "people still do not find these location-sharing technologies all that useful, and they are concerned about their privacy when sharing their locations online." Tsai et al., *supra* at 147. However, "people still believe that the risks of sharing their locations online outweigh the benefits." Tsai et al., *supra*.

limitations on an individual's redress.

Thus, while the EU system provides an adoptable model, these shortcomings should be considered when implementing new data collection legislation in the United States. Accordingly, a successful bill would provide the FTC with more regulatory authority. Such a bill would also need to delineate specific consent and opt-out policies. Finally, any new legislation should include a preemption clause allowing for easier compliance and enforcement.

In 1890, Samuel Warren and Louis Brandeis wrote *The Right to Privacy*, a seminal law review article that called for the creation of privacy rights in an era marked by the invention of photography and the rise of tabloid journalism.[252] In the years that have passed, privacy has morphed into a constitutional right—one that encompasses contraception and abortion.[253] And while privacy within a digital age remains nuanced, there is still a role for regulation. Certainly, there are competing factors—consumer attitudes and the commercial sector's concerns—that must be resolved. Data collection laws, however, can be implemented to provide Americans with broader protection while taking into account consumer attitudes in a modern digital age.

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

253. *See generally* Griswold v. Connecticut 381 U.S. 479 (1965); Roe v. Wade 410 U.S. 113 (1973).