2013

Diminishing Sovereignty: How European Privacy Law Became International Norm

McKay Cunningham
Concordia University School of Law, mccunningham@cu-portland.edu

Diminishing Sovereignty: How European Privacy Law Became International Norm

McKay Cunningham*

* Associate Professor, Phoenix School of Law.

TABLE OF CONTENTS

I. Information and the Internet

There is a tendency to forget how young the Internet is. Modern computing and data trafficking are not even historical pre-teens. The personal computer was not widely available to consumers until the late 1970s, and the Internet was not fully commercialized until 1995.[1] Less than two decades later, seventy-six percent of Americans own at least one personal computer and seventy-seven percent regularly rely on the Internet.[2] Increasingly, businesses, schools, news organizations, and financial institutions offer their services exclusively online.[3] The U.S. Department of Homeland Security reports a high level of integration and reliance, noting that "our economy and national security are fully dependent upon . . . the information infrastructure," and that "the core of the information infrastructure upon which we depend is the Internet."[4]

Not only are business and infrastructure web-reliant, but social interactions are now online affairs. More people spend more time online due to social networking, which represents one of the fastest growing sectors of Internet use.[5] "[T]he time spent on these websites is growing three times faster than the overall Internet rate, and using social networking websites is currently the fourth most popular online activity."[6] Younger demographics more than their senior counterparts eschew traditional forums of social interaction in favor of social

1. *See* Brett Frischmann, *Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market*, 2 COLUM. SCI. & TECH. L. REV. 1, 25 (2001).
2. Internet Usage and Population Growth, INTERNET WORLD STATS, http://www.internetworldstats.com/am/us.htm (last visited Apr. 3, 2013).
3. Jongho Kim, *Ubiquitous Money and Walking Banks: Environment, Technology, and Competition in Mobile Banking*, 8 RICH. J. GLOBAL L. & BUS. 37 (2008) (discussing privacy issues in mobile payments and mobile banking); Edward Lin, *"Virtual" Schools: Real Discrimination*, 32 SEATTLE U. L. REV. 177 (2008); Maurice E. Stucke & Allen P. Grunes, *Toward a Better Competition Policy for the Media: The Challenge of Developing Antitrust Policies That Support the Media Sector's Unique Role in Our Democracy*, 42 CONN. L. REV. 101, 112 (2009).
4. U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE viii (2003), *available at* https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
5. *See News Release: Social Networks & Blogs Now 4th Most Popular Online Activity, Ahead of Personal Email, Nielson Reports,* NIELSEN ONLINE (Mar. 9, 2009), http://www.nielsen-online.com/pr/pr_090309.pdf [hereinafter *Nielsen News Release*]. *See also Social Networking and Blog Sites Capture More Internet Time and Advertising*, NIELSEN NEWSWIRE (Sept. 24, 2009), http://blog.nielsen.com/nielsenwire/online_mobile/social-networking-and-blog-sites-capture-more-internet-time-and-advertisinga/; Dawn C. Nunziato, *Romeo and Juliet Online and in Trouble: Criminalizing Depictions of Teen Sexuality (c u l8r: g2g 2 jail)*, 10 NW. J. TECH. & INTELL. PROP. 57, 58 (2012).
6. Joseph Monaghan, Comment, *Social Networking Websites' Liability for User Illegality*, 21 SETON HALL J. SPORTS & ENT. L. 499, 508 (2011) (citing *Nielsen News Release*, *supra* note 5).

networking sites, leaving those without Internet access outside the social norm.[7] "Increasingly, being connected to society means being connected to the Internet."[8]

Some nations have declared Internet access a fundamental right,[9] claiming that their citizens must be able to access the Internet in order to exercise freedom of expression and other fundamental human rights, providing that states have a responsibility to ensure that Internet access is broadly available. Such protections are not without merit. The uprising in Egypt demonstrated the Internet's vital role in organizing popular revolution as well as the Internet's role in attempts to quash it.[10] Unfortunately, the Egyptian government's decision to truncate Internet access to forestall revolution has been repeated. Syrian officials recently cut Internet access nationwide,[11] a move that may evidence desperation since Internet access is important to both insurgents and establishment alike.[12] If nations, like Egypt and Syria, can sever Internet access to frustrate popular uprisings, declaring such access a fundamental right provides some assurance.

Not only is Internet access and reliance relatively new, its scope is enormous and growing. Wal-Mart, for example, generates more than one million transactions an hour, which requires more than 2560 terabytes. By the end of June 2012, Facebook reported 955 million monthly active users and 552 million daily active users.[13] Twitter estimated over 500 million users and a website that generates "over 400 million tweets a day."[14] Recent YouTube use equates to "500 years of YouTube video are watched on Facebook each day."[15] Approximately 247 billion emails are sent every day.[16] And it is only getting bigger.

---

7. *See Teens on Social Networks*, EMARKETER (Apr. 16, 2009), http://www.emarketer.com/Article/Teens-on-Social-Networks/1007041 (stating that seventy-five percent of American teens use social networks, and predicting that number to increase to seventy-nine percent by 2013). *See also* Amanda Lenhart, *Adults and Social Network Websites*, PEW INTERNET (Jan. 14, 2009), http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx (finding that seventy-five percent of adults, ages eighteen to twenty-four, use online social networks).
8. *See* Jake Adkins, Note, *Unfriended Felons: Reevaluating the Internet's Role for the Purpose of Special Conditions in Sentencing in a Post-Facebook World*, 9 J. TELECOMM. & HIGH TECH. L. 263, 264 (2011).
9. Nicola Lucchi, *Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression*, 19 CARDOZO J. INT'L & COMP. L. 645 (2011); Steven C. Bennett, *The "Right to be Forgotten": Reconciling E.U. and U.S. Perspectives*, 30 BERKELEY J. INT'L L. 161 (2012).
10. *See* James Glanz & John Markoff, *Egypt Leaders Found 'Off' Switch for Internet*, N.Y. TIMES (Feb. 15, 2011), http://www.nytimes.com/2011/02/16/technology/16internet.html (characterizing the internet blackout as "a dark achievement that many had thought impossible in the age of global connectedness").
11. *See* Sean Ludwig, *Internet Shut Down in Syria Amid Mass Protests*, VENTUREBEAT (June 3, 2011), http://venturebeat.com/2011/06/03/internet-shut-down-in-syria-amid-mass-protests/ ("When a Middle Eastern country is in the thick of an uprising, it's almost expected that challenged governments will shut down the Internet to hinder protesters from communicating.").
12. *See* Anupam Chander, Essay, *Jasmine Revolutions*, 97 CORNELL L. REV. 1505, 1520–21, 1524 (2012).
13. *See* Nicole P. Grant, *Mean Girls and Boys: The Intersection of Cyberbullying and Privacy Law and its Social-Political Implications*, 56 HOW. L.J. 169, 180–82 (2012).
14. *Id.* at 181.
15. *Id.* at 182
16. Andrea Bartz & Brenna Ehrlich, *Stop Yourself from Making Egregious E-Mail Errors*, CNNTECH (July 28, 2010), http://www.cnn.com/2010/TECH/social.media/07/28/netiquette.email.mistakes/.

The rate of Internet penetration in developing countries continues to grow. While Internet penetration among many African nations, for example, ranks among the lowest, the growth rate—the rate of new Internet users in Africa—far eclipses the rest of the globe.[17] China added over twenty-seven million Internet users in 2011.[18] At 487 billion gigabytes, the world's digital content reduced to a stack of books would reach to Pluto ten times.[19]

This increasing quantity of information coursing through the Internet spawned a burgeoning industry in data aggregation and analytics. Data mining and analytics generally refer to the collection and analysis of large datasets to divine patterns and relationships among the data that enable enterprises to predict consumer behavior. In 2012, the data collection and analytics industry showed revenues of over $5 billion dollars. A recent study predicts that the "Big Data market is on the verge of a rapid growth spurt that will see it top the $50 billion mark worldwide within the next five years."[20] The field is a large one that is rapidly growing larger, because consumer information is an increasingly valuable commercial asset.

The commercial boom and the benefits inherent in analyzing large amounts of data are offset by a number of concerns including erosion of personal privacy. Much has been written that memorializes and chronicles privacy abuses in the Internet age.[21] A recent empirical study at U.C. Berkeley will suffice for the purposes of this Article as an example of privacy abuse.[22] In 2009 and 2011, researchers gathered data on Internet tracking technologies.[23] Among other findings, they discovered that persistent tracking of personal Internet behavior was not only common but also relatively unknown to consumers.[24] Over two years, the study showed that "the number of tracking cookies expanded dramatically and that advertisers had developed new, previously unobserved tracking mechanisms that users cannot avoid even

17. *See* Idéle Esterhuizen, *Internet Growth Strong in Africa*, ENGINEERING NEWS (Jan. 16, 2012), http://www.engineeringnews.co.za/article/Internet-growth-strong-in-africa-2012-01-16; *Africa Internet Use Hits 2,000 Per Cent Growth*, CITIZEN (Jan. 17, 2012), http://thecitizen.co.tz/business/-/18964-africa-Internet-use-hits-2000-per-cent-growth.
18. *See* Michael Kan, *China Reaches 485 Million Internet Users as Growth Slows*, PC WORLD (July 19, 2011), http://www.pcworld.com/businesscenter/article/235978/china_reaches_485_million_ internet_users_as_growth_slows.html.
19. Richard Wray, *Internet Data Heads for 500bn Gigabytes*, GUARDIAN (May 18, 2009), http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion.
20. Jeff Kelly, *Big Data Market Size and Vendor Revenues*, WIKIBON, http://wikibon.org/wiki/v/Big_Data_Market_Size_and_Vendor_Revenues (last updated Feb. 19, 2013).
21. *See, e.g.*, Andrew Haberman, *Policing the Information Super Highway: Customs' Role in Digital Piracy*, INTELL. PROP. BRIEF, Summer 2010, at 17; Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1318 (2009); Edward J. Eberle, *The Right to Information Self-Determination*, 2001 UTAH L. REV. 965 (2001); Jeffrey B. Ritter et al., *Emerging Trends in International Privacy Law*, 15 EMORY INT'L L. REV. 87 (2001); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173 (1999); Domingo R. Tan, Comment, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661 (1999).
22. Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 273 (2012).
23. *Id.*
24. *Id.*

with the strongest privacy settings."[25] By design, these technologies inhibit consumer choice, obscuring the common practice of monitoring Internet behavior and collecting personal information.[26] In 2010, the Wall Street Journal published several articles highlighting Internet monitoring. One article noted that the "nation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning."[27] As one commentator baldly put it:

> The information that *you* (insert name, address, age, income, and social security number here) read both *Newsweek* and your daily horoscope; buy Häagen-Dazs® ice cream; travel annually to New Mexico; have a standing prescription for Prozac® and buy a variety of different OTC antacids as well as a number of different brands of lubricated condoms; have joined three different health clubs for short sojourns over the past two years; always order a salad in restaurants; never joined Weight Watchers® (and, in fact, have a 31" waist and a body mass index of 25); and give money to public television, is exceedingly valuable for the crassest of reasons: Anyone who has that information can sell it.[28]

Non-consensual harvesting of personal data is not relegated to a few rogue businesses. One estimate reported ninety-two percent of web sites collect personal data.[29] Another industry-funded survey that included 361 web sites and 7500 servers, found that ninety-three percent of those sites collected personal information.[30] Monitoring, recording, collecting, and disseminating private information can now be accomplished with incredible ease, tasks previously impracticable in the pre-Internet age.[31]

The relatively infantile age of information accessibility stemming from the open architecture of the Internet presents policymakers with legal problems that have little precedent outside of awkward and imperfect analogy.[32] How can regulation retain the Internet's benefits

25. *Id. See also* Christine A. Varney, Comm'r, Remarks before the Privacy & American Business National Conference, Consumer Privacy in the Information Age: A View from the United States (Oct. 9, 1996), *available at* http://www.ftc.gov/speeches/varney/priv&ame.shtm (stating that personal information is being collected at rate and to degree unthinkable even five years ago).
26. Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J. LEGAL COMMENT. 393 (2002).
27. Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.
28. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1285 (2000).
29. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (revealing ninety-two percent of 1402 web sites surveyed collected some personal data); Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1164 (2011) (noting that corporate data mining links at least seven thousand transactions to each individual in the United States per year).
30. *See* Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission (June 1999), *available at* http://web.archive.org/web/20040204202945/http://www.msb.edu/faculty/culnanm/GIPPS/gipps1.PDF.
31. *See* Gelman, *supra* note 21, at 1318 ("Most information on the Internet is captured, indexed, saved, and searchable.").
32. *See, e.g.*, Louis John Seminski, Jr., *Tinkering with Student Free Speech: The Internet and the Need for a New Standard,* 33 RUTGERS L.J. 165, 169–70 (2001); Russell L. Weaver, *Speech and Technolo-*

while simultaneously limiting its misuses, an especially daunting task given the Internet's global reach and the impracticability of linking personal data to a certain location, geography and/or jurisdiction?

In this climate, the European Union has emerged as the decisive leader not only for EU Member Nations, but worldwide.[33] Even countries that do not agree with EU policy conform to it.[34] This Article suggests that e-commerce and the Internet spawned a new form of policymaking that enables nations to bend global law without resorting to treaties or other traditional legal tools.

Where the globalization of commerce has been characterized by outsourcing, greater international connectivity and transnational supply chains,[35] the globalization of policymaking finds discrete expression in international data privacy law. The worldwide trend toward national data privacy law provides an interesting and ongoing exemplar of the future of international policymaking. Data privacy law is a complex field wrought with divergent philosophies and ideals that nevertheless is achieving international conformity.[36] At one end of the spectrum, many nations view privacy as essential—a fundamental right enjoyed by their respective citizens.[37] On the other end of the spectrum, data privacy yields to free expression and unregulated commerce.[38] Despite these, and a host of other opposing views, data privacy regulation continues to accelerate both in the number of states adopting national data privacy laws and, perhaps more importantly, in the harmony those laws share with each other.[39] This Article asks how data privacy law, which itself only recently found heightened significance with the rise of the Internet, evolved from a confederacy of dissimilar laws to an evolving harmony of global legislation.

---

gy, 110 PENN ST. L. REV. 703 (2006); Katherine S. Williams, *On-Line Anonymity, Deindividuation and Freedom of Expression and Privacy*, 110 PENN ST. L. REV. 687, 700 (2006).

33. Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655 (2002); Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 BERKELEY J. INT'L L. 939, 956 (2006); Marcia Cope Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 402–05, 454 (2002).
34. *See* Sunni Yuen, *Exporting Trust with Data: Audited Self-Regulation as a Solution to Cross-Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry*, 9 COLUM. SCI. & TECH. L. REV. 41, 18–26 (2008) (detailing the sectoral laws in both India and the Philippines and the subsequent move to national data protection laws); Daniel R. Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement*, 41 CASE W. RES. J. INT'L L. 193, 198–208 (2009). *See generally* Francesca Bignami, *The Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts*, 41 CORNELL INT'L L.J. 211 (2008).
35. *See* Lan Cao, *Corporate and Product Identity in the Postnational Economy: Rethinking U.S. Trade Laws*, 90 CALIF. L. REV. 401, 427–30 (2002).
36. *See* Graham Greenleaf, *Global Data Privacy Laws: Forty Years of Acceleration*, (Univ. of N.S.W. Faculty of Law, Research Series Paper No. 39, 2011), *available at* http://law.bepress.com/cgi/viewcontent.cgi?article=1308&context=unswwps-flrps11.
37. *See, e.g.*, Charter of Fundamental Rights of the European Union pmbl., Dec. 7, 2000, 2000 O.J. (C 364) 1 [hereinafter EU Charter].
38. *See* Leathers, *supra* note 34.
39. *See* Greenleaf, *supra* note 36.

II. Privacy in Europe

A. A Fundamental Right

The contrast between the United States' and European Union's approaches to data privacy illustrates the unlikely harmonization of their laws. In the European Union, data privacy is a fundamental right.[40] While the European Union has long recognized the concept of various fundamental rights, until recently such rights were not native to the European Union, but imported from national constitutions and the European Convention on Human Rights.[41]

It must also be stated that fundamental rights form an integral part of the general principles of law whose observance the Court of Justice ensures. For that purpose, "the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international instruments for the protection of human rights on which the Member States have collaborated or to which they are signatories."[42]

This patchwork of borrowed fundamental rights gave way, in 2000, when the European Union ratified its own statement of fundamental rights—the Charter of Fundamental Rights.[43] Among the rights included in the Charter is the right to privacy.[44] Importantly, the Charter specifies a privacy right in relation to the Internet and modern computing.[45] Under Article 8, Protection of personal data:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[46]

The Charter also recognizes a fundamental right to privacy in general.[47] The historical origins undergirding this commitment to privacy derive in part from Nazi exploitation of European census records preceding and during World War II. Many contend that the extensive accumulation of personal data by the Nazi regime facilitated pre-war abuses of human rights.[48] In 1984, data protection experts concluded that "one of the prime motives for the

40. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1170 (2000); Tracie B. Loring, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421, 423 (2002). *See generally* Andrew T. Hopkins, *The Right to Be Online: Europe's Recognition of Due Process and Proportionality Requirements in Cases of Individual Internet Disconnections*, 17 COLUM. J. EUR. L. 557 (2011).
41. *See* Bignami, *supra* note 34, at 224.
42. *Id.* (citing Case C-305/05, Ordre des barreaux francophones et germanophone v. Conseil des Ministres, 3 C.M.L.R. 28 (2007)).
43. EU Charter, *supra* note 37, pmbl.
44. *Id.* arts. 7–8.
45. *Id.* art. 8.
46. *Id.*
47. *Id.* art. 7 ("Everyone has the right to respect for his or her private and family life, home and communications.").
48. *See* Lynn Chuang Kramer, *Private Eyes Are Watching You: Consumer Online Privacy Protection—Lessons from Home and Abroad*, 37 TEX. INT'L L.J. 387, 397 (2002); Michael W. Heydrich, Note, *A*

creation of data protection laws in continental Europe is the prevention of the recurrence of experiences in the 1930s and 1940s with Nazi and fascist regimes."[49] Such abuse in recent history of private and personal information undergirds European vigilance in "protecting personal privacy and resisting state intrusions into private life."[50]

A few years after World War II, the United Nations adopted the Declaration of Human Rights, a document that laid a foundation for legal protection of privacy rights. The Declaration provided that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."[51] Several European nations enacted a series of privacy and data protection laws in the following decades. Sweden became the first nation to enact a comprehensive national data privacy law with its Data Act of 1973.[52] In 1973 and 1974, the Council of Europe's intergovernmental body passed resolutions recommending that member states adopt data protection laws.[53]

In the 1980s non-governmental organizations like the Organization for Economic Cooperation and Development (OECD) attempted to articulate legal principles governing data privacy that could be widely implemented and perhaps unify divergent national laws.[54] These guidelines initially proved fruitless. The problem ultimately forced resolution. Multiple and conflicting privacy laws within Europe motivated the harmonization of privacy law, given that conflicting privacy laws discourage commerce and the free flow of information from one nation to the next.[55] Over fifteen years after the OECD articulated proposed data privacy guide-

---

Brave New World: Complying with the European Union Directive on Personal Privacy through the Power of Contract, 25 BROOK. J. INT'L L. 407, 417 (1999).

49. COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 1, 30 (1992) (quoting David H. Flaherty, *Nineteen Eighty-Four and After*, 1 GOV'T INFO. Q. 431 (1984)).
50. Lee Dembart, *The End User/A Voice for the Consumer: Privacy Undone*, N.Y. TIMES (June 10, 2002), http://www.nytimes.com/2002/06/10/business/worldbusiness/10iht-itend10_ed3_.html.
51. Universal Declaration of Human Rights art. 12 G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).
52. David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 95 (1999). *But see* Heydrich, *supra* note 48, at 417 (suggesting that the United States originated the right to privacy and that the first data privacy legislation was passed in the German state of Hesse in 1970).
53. *See* Council of Europe, Comm. of Ministers, Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, 224th Mtg., Res. (73) 22 (Sept. 26, 1973), *available at* https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2; Council of Europe, Comm. of Ministers, Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, 236th Mtg., Res. (74) 29 (Sept. 20, 1974), *available at* https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2.
54. The Organization for Economic Co-operation and Development (OECD) is an international economic organization of over thirty countries founded in 1961 to stimulate economic growth and world trade. It was originated in 1947 to run the U.S.-financed Marshall Plan for reconstruction of a war-torn continent. *History*, OECD, http://www.oecd.org/about/history/ (last visited Apr. 5, 2013). For background information on OECD, see BENNETT, *supra* note 49, at 136–40.
55. *See* Patrick J. Murray, Comment, *The Adequacy Standard under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 FORDHAM INT'L L.J. 932, 949–51 (1998).

lines, those guidelines would largely become the template for binding legislation throughout Europe.[56]

In 1990, the Commission of the former European Community drafted a proposed Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data.[57] After some revision, the European Parliament approved the draft Directive on March 11, 1992,[58] and the elusive goal of European unity with regard to data privacy law grew closer with the formal enactment of Council Directive 95/46/EC on October 24, 1995.

B. The European Union Directive

The 1995 European Directive marked a sea of change in the previously elusive attempts at unifying data privacy law in Europe. Although almost twenty years old, the Directive remains the single most impactful data privacy law worldwide.[59] The Directive's twin purposes seek to (1) protect fundamental privacy rights, and (2) promote the "free flow of personal data between Member States."[60] To do so, the Directive imposes restrictions on organizations that process personal data and grants rights of access and correction to "data subjects"—EU residents protected by the Directive.[61]

Specifically, the Directive requires each of the European Union's twenty-seven Member States to pass a privacy law that encompasses both government and private entities that process personal data.[62] These national laws are not relegated to specific industries, such as the medical or financial industries, but reach all processing of data relating to an EU resident's personal information.[63] Data processors must comply with a number of "data quality principles." Personal data must be: (a) processed fairly and lawfully; (b) collected for legitimate and specified reasons; (c) adequate, relevant and not excessive in relation to the purposes for which it is collected; (d) accurate and, where necessary, kept up to date; and, (e) retained as identifiable data for no longer than necessary to serve the purposes for which the data were collected.[64]

These requirements may appear harmless, but they implicate a world of transactions: they would arguably bar a bank from reviewing its own customer files for good prospects, limit market estate planning services, as well as restrict an employer from keeping records or

56. *See* Kramer, *supra* note 48, at 390 (citing JOHN DICKIE, INTERNET AND ELECTRONIC COMMERCE LAW IN THE EUROPEAN UNION 55–64 (1999)).
57. *Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network (ISDN) and Public Digital Mobile Networks*, COM (1990) 314 final (July 27, 1990).
58. European Parliament and Council Directive 95/46/EC, art. 5, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [hereinafter Data Protection Directive].
59. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 55–88 (2000); Ryan Moshell, Comment, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 384 (2005).
60. *See* Data Protection Directive, *supra* note 58, art. 1.
61. *Id.*
62. *Id.*
63. *Id.* art. 8.
64. *Id.* art. 6.

backup files for several years.[65] If relegated to the twenty-seven Member States of the European Union, these requirements may indeed seem innocuous, but the Directive's reach far exceeds its grasp.[66] While the European Union has no jurisdiction to directly bind those states outside its union, the Directive endeavors to do so anyway.[67] It does so (1) by broadly defining "processing personal information"[68] and (2) by prohibiting transfers of personal data to entities that fail to ensure an "adequate level of protection."[69]

1. Processing Personal Information

The Directive's wide-ranging breadth and reach find expression in the definitions of those who must comply.[70] Three definitions, all generous in scope, capture more than they exclude: The Directive applies to (1) personal data, that is (2) processed by (3) controllers or processors. "Personal data" is defined in the Directive as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[71]

Personal data is not limited to a lay understanding. It includes more than names, national identification numbers, bank accounts, and addresses.[72] It encompasses information that can lead to identification directly or indirectly. Labeled an "expansionist view," it is "irrelevant if information has already been linked to a particular person, or might be so linked in the future; this view treats identified and identifiable data as equivalent."[73] Data becomes personal information when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link.[74]

The Data Protection Working Party, a representative body drawn from EU Member States and charged with fostering consistent interpretation of the Directive's requirements, issued an opinion in 2007 clarifying the definition of personal information.[75] The Working Party determined that a person is "identifiable" when, "although the person has not been identified

65. Donald C. Dowling, Jr., *Global HR Hot Topic—May 2007: Global HRIS and EU Data Privacy Law Compliance*, GLOBAL HR HOT TOPIC (Case & White LLP, New York, N.Y.), May 2007, *available at* http://www.whitecase.com/hrhottopic_0507/#.UV4hE6KiYbQ.
66. Robert Browning wrote that a person's "reach should exceed his grasp, [o]r what's a heaven for?" JOHN BARTLETT, FAMILIAR QUOTATIONS 542–43 (15th ed. 1980).
67. *See* Christopher Kuner, *Beyond Safe Harbor: European Data Protection Law and Electronic Commerce*, 35 INT'L LAW. 79, 87 (2001).
68. Data Protection Directive, *supra* note 58, art. 2(a).
69. *Id.* pmbl. recital 57, art. 25(1).
70. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011).
71. Data Protection Directive, *supra* note 58, art. 2(a).
72. *See* Schwartz & Solove, *supra* note 70, at 1819.
73. *See id.* at 1817 (arguing that information privacy regulations rest on an unstable and ill-defined concept of personally identifiable information).
74. *Id.*
75. *See* Data Prot. Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN, WP 136 (June 20, 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

yet, it is *possible* to do it."[76] Information need not identify an individual with specificity to constitute "personal data;" the mere fact that the information is related to an individual capable of being identified qualifies it as "personal data" under the Directive.[77] One commentator has suggested that "anyone who posts personal information about another person on his or her own social networking profile or uses personal information from another person's profile could be deemed a 'data controller' subject to the data protection obligations of the Directive."[78]

The Directive combines the broad definition of personal data with a broad definition of "data processing:" "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[79]

Any collection, use, and transfer—even the redaction and deletion thereof—constitutes "processing."[80] This definition intentionally encompasses data processed automatically as part of a filing system.[81] The Directive defines those deemed to have "processed" personal data as either data controllers or data processors. A data controller is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[82] Data controller, thusly defined, captures more than big businesses and data aggregators like Corelogic, Datalogix, EBureau, and ID Analytics. As one commentator notes, children recording orders for Girl Scout cookies, individuals organizing their business contacts, and students operating websites that require registration all qualify as data controllers.[83]

These purposefully broad definitions capture a wide array of organizations that "process" "personal data."[84] But entities and individuals outside the twenty-seven Member States of the European Union might claim exemption from its jurisdictional reach. The Directive, however, encompasses a surprisingly broad range of non-E.U. entities by forbidding transfers of personal data.

2. Data Transfers

"Because of its potential effect on other nations that interact with or do business in Europe, [the data-flow restriction] may be the most controversial feature of the Directive."[85] The Directive levies significant restrictions on those entities in the European Union that process

76. *Id.*
77. PRIVACY AND DATA SECURITY LAW DESKBOOK § 18.02[A] (Lisa J. Sotto ed., 2010).
78. Bennett, *supra* note 9, at 186.
79. Data Protection Directive, *supra* note 58, art. 2(b).
80. *Id.*
81. *Id.* pmbl. recital 15, art. 5.
82. *Id.* art. 2(d).
83. *See* Cate, *supra* note 21, at 183.
84. *See* Schwartz & Solove, *supra* note 70.
85. Steven R. Salbu, *Regulation of Borderless High-Technology Economies: Managing Spillover Effects*, 3 CHI. J. INT'L L. 137, 137 (2002).

personal information.[86] This added cost of business had potential for creating unintended yet foreseen consequences, namely incentivizing companies to outsource data processing beyond E.U. borders.[87] A company doing business in Spain might decide, for example, to relocate its principle place of business outside the European Union to avoid the cost of complying with the Directive. To forestall such an exodus, Article 4 of the Directive extends its reach to "equipment" within a Member State.[88]

Each Member State shall apply the national provisions it adopts pursuant to the Directive to the processing of personal data where "the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."[89]

This provision not only dissuades EU companies from relocating, it also reaches a host of non-EU entities. Many organizations headquartered in countries outside the European Union have been surprised to learn of their obligation to comply with EU law. A U.S. company based in Ohio engaged in e-commerce must comply with the Directive if that company uses "cookies" to sell items online and has even one EU customer.[90] A cookie, generally understood, installs a program on the consumer's computer that tracks and remembers transactions.[91] The shopping cart icon that "remembers" what a customer selects and puts those selections in a virtual shopping cart serves as a common illustration.[92] Because an EU customer's computer is used in the transaction due to the "cookie" installed on that computer, EU-based "equipment" is used for the purpose of processing personal data and the strictures of the Directive apply.[93] The national law of the Member State in which the customer's computer is located governs the data processing conducted by the Ohio company.

Many have criticized this provision as overreaching, especially when applied to non-EU based entities processing intra-company data housed outside the European Union.[94] Such criticisms do not solely target the "equipment" provision outlined above because the Directive includes additional restrictions on data transfers that are arguably more intrusive. In other words, the Directive's reach does not stop with data processing that uses EU-based "equip-

86. *Id.* at 140–41.
87. *See* PRIVACY AND DATA SECURITY LAW DESKBOOK, *supra* note 77, § 18.02[A][1][c].
88. Data Protection Directive, *supra* note 58, art. 4.
89. *Id.* art. 4(c).
90. *See* Hoofnagle et al., *supra* note 22, at 276 ("One way that websites track users is through 'cookies,' small text files that typically contain a string of numbers that can be used to identify a computer. For instance, a website might set a tracking cookie on a user's computer with a key (a fancy word for the cookie name) such as 'id' and value (the unique identifier assigned to a user) such as '123456789.' Advertisers can then access the 'id' cookie and track how user 123456789 visits different websites.").
91. *See id.*
92. Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281 (2012).
93. *See* PRIVACY AND DATA SECURITY LAW DESKBOOK, *supra* note 77, § 18.02[A][1][c].
94. *See, e.g.*, Kuner, *supra* note 67, at 87.

ment."[95] The Directive specifically targets data transfers to "third countries," outlining a host of requirements before personal data can leave Europe.[96]

Article 25, in fact, baldly prohibits the transfer of personal data to a third country (any Non-EU or European Economic Area (EEA) country) unless the European Commission ("Commission") deems that country has an "adequate level of protection."[97] Data about EU residents can only go to those countries that have enacted data protection laws that the Commission deems "adequate."[98] Given the broad definition of "personal information," the global economy, and the free flow of data over the Internet, this restriction appears unmanageable at best. The Commission currently recognizes only nine countries as adequately compliant: Andorra, Argentina, Canada, Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, and Switzerland.[99]

To join this very short list, the Commission conducts a formal evaluation of the transferee country's laws and practices. The transferee country "shall be assessed in the light of all the circumstances surrounding a data transfer," including the nature of the data, the purpose and duration of the proposed processing, the "rules of law, both general and sectoral," in the transferee country, and the "professional rules and security measures which are complied with in that country."[100] The formal designation as "adequate" allows transmission of personal data from France to Argentina as if the same information was transferred from France to Spain.[101] Again, only nine countries have met the standard.

The heart of this Article suggests that the European Union, through the Directive, is forcing international compliance even from nations that would resist it. If only nine nations comply with the Directive in a manner sufficient to meet the EU standard, how does the Directive ensure compliance from the rest of the international community? Does this mean that data about EU residents can only exist within the EU and nine random countries?

---

95. Data Protection Directive, *supra* note 58, art 25.
96. *Id.*
97. *Id.* art. 25(1).
98. *Id.*
99. *See* Greenleaf, *supra* note 36, at 3 n.2.
100. Article 25(2) of the Directive articulates five factors: (1) the nature of the data, (2) the purpose and duration of the processing operation, (3) the country of origin and the country of final destination, (4) the rule of law in force in the third country, and (5) the professional rules and security measures adhered to and implemented by the receiving entity in the third country. Data Protection Directive, *supra* note 58, art. 25(2). The prohibition in Article 25 is subject to exemptions, provided in Article 26, when (1) the data subject has consented "unambiguously" to the transfer; (2) the transfer is necessary to the performance of a contract between the data subject and the controller or of a contract in the interest of the data subject concluded between the controller and a third party; (3) the transfer is legally required or necessary to serve an "important public interest;" (4) the transfer is necessary to protect "the vital interests of the data subject;" or (5) the transfer is from a "register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest." *Id.* art. 26.
101. *Id.*

3. Enabling Transfers That Conform

As mentioned, the Directive forbids transfer of EU personal data to countries like the United States because the Commission finds U.S. data protection laws inadequate; that is, unless "adequacy" can be established by other means.[102] In practice, the adequacy requirement has been relaxed to apply on an ad hoc individual basis, rather than by nationality. Three avenues[103]—outside of a formal nationwide adequacy finding—allow non-EU entities to receive and process EU personal data: (1) binding/model contracts, (2) binding corporate rules, and (3) safe harbor self-regulation.[104]

Model contracts allow legal transmission of personal data outside of Europe by requiring "binding," "standard," or "model" contractual clauses.[105] The Directive empowers the Commission to approve transfers of personal data even to third countries that fail to ensure an "adequate level of protection" if the data controller erects "sufficient safeguards" via "certain standard contractual clauses" consistent with a "Commission's decision."[106] Under this approach, the contractual clauses incorporate by reference the data protection laws of the Member State in which the data exporter is established.

---

102. Donald C. Dowling, Jr., *International Data Protection and Privacy Law*, INT'L EMP. PRAC. (Case & White LLP, New York, N.Y.), Aug. 2009, at 10 ("Under a strict reading of the Directive's article 25(1), personal data transmissions to any other country would appear flatly illegal. . ."), *available at* http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf.

103. The Directive's article 26(1) authorizes a number of other exceptions legally to transmit personal data outside of Europe even to a "third country" that fails to offer an "adequate level of protection." Data Protection Directive, *supra* note 58, art. 26(1). A data controller or processor can legally send personal data outside of Europe to the United States, or any other country, if:

> (a) the data subject has [freely] given his consent unambiguously to the proposed transfer [to be enforceable, a consent must indeed be unambiguous and freely given; EU data authorities take the position that a consent must specifically list the categories of data and the purposes for the processing outside the EU; in the employment context, consents may be deemed presumptively not freely given, merely because of the imbalance in bargaining power between employer and employee]; or
>
> (b) the transfer is necessary [not merely convenient] for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
>
> (c) the transfer is necessary [not merely convenient] for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
>
> (d) the transfer is necessary [not merely convenient] or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (e) the transfer is necessary [not merely convenient] in order to protect the vital interests of the data subject; or
>
> (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Id.

104. *See* Leathers, *supra* note 34, at 199–200.

105. *See* Data Protection Directive, *supra* note 58, art. 26(4).

106. *Id.*

Binding corporate rules function similarly, but serve a more permanent, less ad hoc purpose.[107] Binding corporate rules track EU data protection standards and allow multinational organizations to conduct business with EU counterparts without having to draw up model contract language for every transaction.[108] The relevant Member State's data protection agency must approve binding corporate rules, which can be an arduous and lengthy process.[109] As a result, relatively few binding corporate rules have been approved.[110]

4. Safe Harbor: The American Exception

Finally, organizations and individuals in the United States can comply with the Directive and thereby receive and process personal data from the European Union if they self-certify under the Safe Harbor provision. The Safe Harbor provision—available only in the United States—represents a compromise between EU and U.S. regulators.[111] As laid out below, the United States' aversion to data privacy regulation, coupled with uneven enforcement, undermines the European Union's view of data privacy as a fundamental right.

The Directive drew a hard line by outlawing data transfers to any third country that fails to offer "adequate" data protection, presenting a live threat to U.S.-based companies reliant on data from their own European employees, customers, suppliers, and associates.[112] The European Union has not waivered from its characterization of U.S. privacy law as "inadequate" to protect privacy rights because of U.S. piecemeal privacy regulations.[113] It is not difficult to imagine the range of transactions affected by such a severe restriction of data. A U.S. multinational company with employees or customers in the European Union would have to pull down or drastically restructure interactive websites and company intranets, stop customer reservations, delete frequent-customer databases, discontinue customer help lines, discard customer and employee directories, discontinue routine financial transactions including credit card transactions and check-clearing, and overhaul or discontinue routine mail, express delivery documents, e-mails, and telephone calls. "As soon as the Directive became effective in 1998, it became clear that it actively threatened data flows between the two largest trading partners on Earth."[114] As one commenter put it, such action "would immediately destroy a $1.5 trillion transatlantic economic relationship."[115]

The U.S. Department of Commerce and the European Commission bargained for two years before agreeing to a "Safe Harbor" exception in 2000, avoiding serious disruption be-

107. This option was created by the Data Protection Working Party, which is an advisory body that was created by article 29 of the Data Directive. *See* Data Protection Directive, *supra* note 58, art. 29.
108. *See* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 14-3 (Christopher Wolf ed., 2007).
109. *See* PRIVACY AND DATA SECURITY LAW DESKBOOK, *supra* note 77, § 18.02[B].
110. *See id.*
111. *See* Leathers, *supra* note 34.
112. *See* Data Protection Directive, *supra* note 58, art. 25.
113. *See* Leathers, *supra* note 34, at 198.
114. Dowling, *supra* note 102.
115. *See* Stephen R. Bergerson, *Electronic Commerce in the 21st Century: Article E-Commerce Privacy and the Black Hole of Cyberspace*, 27 WM. MITCHELL L. REV. 1527, 1550 (2001).

tween the trading partners.[116] The compromise sought to bridge the differing approaches in the European Union and the United States, simplify the means for U.S. organizations to comply with the EU Directive, and shield EU organizations that transfer personal data to U.S. organizations.[117] Eligibility for Safe Harbor protections requires U.S. organizations to be subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation.[118] The Safe Harbor requirements themselves largely track the Directive's requirements, although not precisely.[119]

The Safe Harbor privacy principles are essentially those required by the Data Directive: (1) notice; (2) choice; (3) onward transfer; (4) security; (5) data integration; (6) access; and (7) enforcement.[120] Consequently, it appears that the Safe Harbor provision merely mirrors the Directive, raising the query: How is the Safe Harbor a "compromise" between EU regulators intent on forcing U.S. compliance with the Directive and U.S. officials anxious to avoid the same? The compromise is embodied by the voluntary and largely self-regulatory implementation of these data protections.[121]

Companies that apply for Safe Harbor self-certify that they comply with the restrictions listed above. No government official reviews or authorizes whether any given company in fact complies with Safe Harbor principles before awarding certification.[122] Instead, the Department of Commerce keeps an online list of entities that certify their compliance with Safe Harbor.[123] A company need only notify the U.S. Department of Commerce that it intends to comply with Safe Harbor and publicly declare compliance on its website.[124]

---

116. *See U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, EXPORT.GOV, http://www.export.gov/safeharbor (last updated Apr. 11, 2012, 2:45 PM) [hereinafter *Safe Harbor Frameworks*]; *see also* documents adopted by the Data Protection Working Party 1999, http://ec.europa.eu/justice/data-protection/document/index_en.htm.
117. *See Safe Harbor Frameworks*, *supra* note 116.
118. *See Safe Harbor Overviews*, EXPORT.GOV, http://www.export.gov/safeharbor/eg_main_018236.asp.
119. Kamaal Zaidi, *Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 MICH. ST. J. INT'L L. 169, 170 (2003) ("Using the EU Directive's principles, the Safe Harbor creates a scheme by which U.S. companies are required to comply with stricter privacy standards relating to the transfer of online personal data. With respect to U.S. privacy law, this Safe Harbor regime substitutes the predominant sectoral approach with a more comprehensive approach."). *But see* Morey Elizabeth Barnes, Comment, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 NW. J. INT'L L. & BUS. 171, 182 (2006) (suggesting EU officials may soon "reconsider whether the Safe Harbor really mirrors the letter and spirit of the Data Privacy Directive").
120. *See* PRIVACY AND DATA SECURITY LAW DESKBOOK, *supra* note 77, § 18.02[B].
121. *See* Leathers, *supra* note 34, at 201 ("The Safe Harbor is a voluntary self-certification system that is unique to the U.S. . . . .").
122. *See U.S.-EU Safe Harbor List*, EXPORT.GOV, https://safeharbor.export.gov/list.aspx ("In maintaining the list, the Department of Commerce does not assess and makes no representations to the adequacy of any organization's privacy policy or its adherence to that policy. Furthermore, the Department of Commerce does not guarantee the accuracy of the list and assumes no liability for the erroneous inclusion, misidentification, omission, or deletion of any organization, or any other action related to the maintenance of the list.") (last visited Apr. 5, 2013).
123. *See id.*
124. *Id. See also* PRIVACY AND DATA SECURITY LAW DESKBOOK, *supra* note 77, § 18.02[B].

5. Safe Harbor: Compromise and Criticism

Neither the European Union nor the United States fully embrace the Safe Harbor provision. While the European Union views privacy as a fundamental right, safeguarded by the Directive and directly administered and enforced by public authorities, U.S. officials view data privacy as a matter of compromise, and advocate private-sector self-regulation as the best method of enforcing privacy principles.[125]

EU officials criticize self-regulation, noting that many of the few organizations that have self-certified do not in fact comply with Safe Harbor principles. Two years into the Safe Harbor agreement, an EU Commission issued a working paper that reported significant noncompliance.[126] Many U.S. companies that claimed to protect private data lacked "the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies."[127] The Commission found that U.S. companies often failed to display the mandatory public statement of adherence to the Safe Harbor principles, and that many of the privacy statements that the Commission did locate inaccurately reflected Safe Harbor principles.[128] The Commission concluded that "less than half of organisations post privacy policies that reflect all seven Safe Harbor Principles."[129]

Finally, only a fraction of U.S. entities eligible for Safe Harbor have sought certification. A significant block of companies that would suffer "severe, adverse effects" if data transfers from the European Union were blocked have ignored the Safe Harbor altogether.[130] "U.S. firms, even those within the Safe Harbor, are largely ignoring data-protection standards."[131] As of October 2006, approximately 1000 companies were participating in the program, 190 of which were "not current" in their certification.[132] Given the cost of implementing data privacy controls and the concomitant risk of prosecution,[133] questions remain regarding whether

125. Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now Is the Time*, 1 CASE W. RES. J.L. TECH. & INTERNET 1, 7 (2009).
126. Commission Decision 2000/518/EC, 2000 O.J. (L 215) 1, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0001:0003:EN:PDF [hereinafter Commission Decision 2000/518/EC].
127. *Commission Staff Working Paper*, at 2, SEC (2002) 196 (Feb. 13, 2002).
128. *Id.*; Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500 (1995) ("Despite the growth of the Information Society, the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector. Legal rules have developed on an ad hoc, targeted basis, while industry has elaborated voluntary norms and practices for particular problems. Over the years, there has been an almost zealous adherence to this ideal of narrowly targeted standards." (footnotes omitted)).
129. *Commission Staff Working Paper*, *supra* note 127, at 9.
130. Barnes, *supra* note 119, at 181.
131. Moshell, *supra* note 59, at 387 (citing Adam Eisner, *U.S. Firms Still Ignoring EU Privacy Regulations*, THEWHIR.COM (Aug. 14, 2003), http://www.thewhir.com/web-hosting-news/us-firms-still-ignoring-eu-privacy-regulations).
132. Barnes, *supra* note 119, at 181–82.
133. *See* Loring, *supra* note 40, at 459 ("The unwillingness of U.S. organizations to participate in the safe harbor can be attributed to factors such as uncertainty over enforcement issues, compliance costs, and a reluctance to be one of the first organizations to test the safe harbor. In addition, organizations may not be subscribing to the safe harbor because the EU Directive has no authority outside of Europe." (footnotes omitted)).

more U.S. organizations will self-certify, and whether those that have self-certified will in fact comply.[134]

Aside from criticisms involving self-certification, many privacy advocates lament the Safe Harbor enforcement scheme. In the European Union, the Directive requires enforcement solely through government agencies.[135] The Data Protection Authority in each EU Member State enforces its respective data privacy law.[136] In fact, some Member States require all data collectors and processors to file annual reports.[137] Conversely, enforcement of U.S. Safe Harbor provisions involves a number of self-regulatory stages before meaningful government intervention ensues, leading one scholar to note that "[p]rivate-sector enforcement is the principal method of assuring compliance with the Safe Harbor Principles."[138]

The first enforcement stage involves self-certification. Organizations may either conduct a self-assessment or hire a third party to verify certification.[139] Third party assessors, like BBB Online or TRUSTe, certify that the organization has a properly posted privacy policy, that the policy adheres to Safe Harbor provisions, and that the organization in fact complies with its own policy.[140] Private-sector enforcement calls for implantation of a dispute resolution system to investigate and reconcile consumer complaints and empowers the mediator, arbitrator or other dispute resolution body with the ability to sanction an organization that cannot demonstrate the required level of privacy protection.[141]

As a result, an EU resident concerned about her personal data must first contact the U.S. company directly. The complainant could then pursue a grievance by contacting the third party company that verified compliance with the Safe Harbor provisions and argue that the company failed to adhere to its own privacy policy.[142] If the third party agrees with the complainant, it directs the company to remedy the infraction. If the company fails to do so, the third party must refer the case to the agency with jurisdiction, invariably the FTC.[143] Even then, the FTC has discretion whether or not to investigate.[144] EU officials, dissatisfied with Safe Harbor provisions, note that it took the FTC nine years to bring its first data privacy en-

134. *See* David Raj Nijhawan, *The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939, 945 (2003) (noting that U.S. businesses see self-certification as creating more problems than not joining).
135. Data Protection Directive, *supra* note 58, art. 28.
136. *See id.* art. 28(1).
137. *See* Leathers, *supra* note 34, at 206 ("Some EU member states' Data Protection Authorities require all data collectors and processors to file annual reports.").
138. Loring, *supra* note 40, at 455.
139. *See* Leathers, *supra* note 34, at 206–07 (noting that enforcement under Safe Harbor provides a multiple "layer" approach wherein the first enforcement "layer" is the initial Safe Harbor registration and subsequent annual Safe Harbor registration renewals, run by the DOC followed by an "independent recourse mechanism" before the final "layer" of government intervention).
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *See id.* at 195–96.

forcement action.[145] The FTC prosecuted a U.S. company that misrepresented its compliance with Safe Harbor principles.

Although Safe Harbor provisions require U.S. entities to treat EU personal data as if that data were physically in Europe and subject to the Data Directive,[146] the Safe Harbor is a voluntary self-certification system that is unique to the United States and arguably suffers from inadequate enforcement.[147] The private sector remains reluctant to implement Safe Harbor principles, and many of the few companies that have self-certified do not in fact comply with Safe Harbor principles.[148]

C. International Trend

This Article's central premise asks how the European Union forced international compliance with its data privacy Directive, a regulation described by one scholar as "the most rigorous privacy legislation the world has seen."[149] That query requires an understanding of European history and the subsequent adoption of privacy as a fundamental right. The Directive is the legal codification of this deep-seated belief, providing a range of protections for EU residents and their private data.[150] Private data, however, knows no borders in the Internet age.[151] Private data is no longer confined to paper dossiers and metal file cabinets, but can be many places at once, travel at light speed from one nation to the next, and can be readily collected without notice or consent.

As private data operates without borders, so must the Directive. It is this component of the Directive that bears emphasis especially in light of the seeming success obtained in securing international conformity.[152] Broad and encompassing definitions of "personal information" and data "processing," in conjunction with restrictions on data transfers, encourage international compliance at the risk of exclusion from the European market.[153] The Directive allows

145. *Id.* ("[S]ince the Safe Harbor's inception, the program has been subject to heavy criticism from privacy advocates and an EU oversight committee. The heaviest criticism is levied against the Safe Harbor's inadequate internal and external enforcement mechanisms." (footnotes omitted)). *See also* News Release, Fed. Trade Comm'n, Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site (Aug. 6, 2009), *available at* http://www.ftc.gov/opa/2009/08/bestpriced.shtm.

146. *See* Leathers, *supra* note 34, at 201.

147. Moshell, *supra* note 59, at 384 ("Taken as a whole, the U.S. system of self-regulation of data protection has proved to be fundamentally flawed. Without legislation that provides a solid support structure for what little government data-protection authority exists, the United States suffers from a general lack of enforcement that stems from industry disregard for voluntary data-protection concepts." (footnotes omitted)).

148. Salbu, *supra* note 85, at 137. *See also id.* at 139–40 (noting that "some observers believe that the U.S. Safe Harbor principles are weak and meaningless, and do not go nearly far enough, while others see them as an intolerable European incursion into sovereignty and autonomy").

149. *Id.* at 137.

150. *See* Leathers, *supra* note 34, at 197–98 ("In contrast to the U.S. 'sectoral' approach to privacy, the EU 'omnibus' approach to privacy regulation views privacy as an ends with respect to its inherent nature; the EU views privacy as a protected state-of-being that is representative of individual autonomy.").

151. *See* Michael Geist, *Cyberlaw 2.0*, 44 B.C. L. Rev. 323 (2003); JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 188 (2008).

152. *See* Salbu, *supra* note 85.

153. *Id.*

data transfers both on a national and an ad hoc basis, but only after binding the transferee to the data protections articulated in the Directive.[154]

Although many nations have not historically embraced privacy as a fundamental right, the clear trend in global privacy law reflects an increasing adherence to EU privacy principles.[155] The first comprehensive national data privacy law, Sweden's Data Act of 1973, marked the beginning. The forty years that followed produced at least seventy-five more nations adopting similar national data privacy laws. "The picture that emerges is that data privacy laws are spreading globally, and their number and geographical diversity accelerating since 2000."[156] There were seven new national omnibus privacy laws in the 1970s, ten in the 1980s, nineteen in the 1990s, thirty-two in the 2000s and eight so far in the first two years of this decade.[157] At the current rate of expansion, fifty new laws will emerge in this decade.[158] The most economically significant nations notably absent are China and the United States. The Directive's initial success in swaying international compliance is by no means complete. The United States has long resisted comprehensive data privacy laws, and its beleaguered economy seeks to optimize those industries—like data aggregation and analytics—that show promise. The next five years will reveal whether the Directive's reach will flip U.S. reluctance into begrudged acceptance, or at last meet an obstacle that cannot be moved.

III. Privacy in America

The centralized approach exemplified by the European Union favors data protection accomplished by comprehensive legislation. By contrast, data protection laws in the United States are decentralized, fragmented, industry-specific, and largely uncoordinated among varying levels of government.[159] "While the European Union enacts legislation to counter market forces, the United States, in comparison, focuses less on government intervention in the private sector and, instead, places a greater emphasis on market constraints."[160] The European approach is comprehensive, proactive, and preventative, whereas the United States relies on a salmagundi of laws including provisions in federal and state constitutions, federal and state statutes, federal and state regulations, common law, municipal ordinances, and self-regulatory practices.[161] This disjointed and largely reactive compendium of privacy regulation has earned the widely-used moniker "sectoral."[162]

154. *See* Leathers, *supra* note 34, at 199–200.
155. *See* Yuen, *supra* note 34, at 18–26 (2008) (detailing the sectoral laws in both India and the Philippines and the subsequent move to national data protection laws).
156. Greenleaf, *supra* note 36, abstract.
157. *Id.*
158. *Id.*
159. Murray, *supra* note 55.
160. Loring, *supra* note 40, at 425—26.
161. *See* David A. Tallman, *Financial Institutions and the Safe Harbor Agreement: Securing Cross-Border Financial Data Flows*, 34 LAW & POL'Y INT'L BUS. 747, 755 (2003); Abraham Shaw, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 519–20 (2010); Mark Silverstein, *Privacy Rights in State Constitutions: Models for Illinois?*, 1989 U. ILL. L. REV. 215, 216–17 (1989).
162. *See generally*, Cate, *supra* note 21 (noting many and disparate privacy related statutes).

The industries beholden to data protection legislation are those that traditionally handle sensitive data,[163] and the laws are often customized, targeting discrete elements of sensitive data or particular uses thereof.[164] Examples of the U.S. sectoral approach include the Telecommunications Act of 1996, which restricts telecommunications carriers' use of private customer information;[165] the Gramm-Leach-Bliley Act, which restricts financial institutions' use and dissemination of private financial data;[166] and the Fair and Accurate Credit Transactions Act, which restricts credit reporting and increases protections for related personal information.[167] Whereas the European Directive articulates a single definition of personal information that governs its twenty-seven Member States,[168] the U.S. sectoral approach breeds multiple, often disparate, definitions. The definition of personal data under the Fair Credit Reporting Act,[169] for example, differs from the Video Privacy Protection Act,[170] which differs from the Gramm-Leach-Bliley Act.[171]

The self-regulatory aspect of U.S. data privacy protections emerges most clearly through the Safe Harbor provisions discussed above. Another self-regulatory industry separate from the Safe Harbor exists in credit card privacy regulation. The credit card industry requires companies that store, process, or transmit credit card information to institute and enforce a security policy, encrypt specified credit card information, and report lost data.[172]

All told, the United States certainly legislates and enforces an array of privacy protections. Those protections, however, are not uniform and comprehensive but instead resemble an uncoordinated patchwork of sectoral privacy laws.[173] Efforts to unify data privacy laws by enacting comprehensive legislation have been consistently rejected.[174] Many project that a comprehensive data privacy law is unlikely in the near term,[175] a projection that highlights U.S. aversion to comprehensive data privacy regulation. Perhaps an industry-specific and self-regulatory approach to data privacy is superior to national, omnibus regulation. In considering whether the European Directive, coupled with the international trend favoring national privacy legislation, will eventually catch up and envelope the United States, it is important to examine the U.S. rationale for resisting the same.

---

163. *See* PRIVACY AND DATA SECURITY LAW DESKBOOK, *supra* note 77, § 1.01.
164. *Id.*
165. Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat 56 (codified at 47 U.S.C. § 151 et seq. (1996)).
166. Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801–09 (1999).
167. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 (2006).
168. *See* Data Protection Directive, *supra* note 58, art. 2.
169. FCRA § 1681(b) (applying to consumer reporting agencies that provide consumer reports, defined as communications by such an agency bearing on a consumer's credit worthiness or personal characteristics when used to establish consumer's eligibility in certain contexts).
170. Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2002) (defining personally identifiable information as "information which identifies a person").
171. Gramm-Leach-Bliley Act of 1999, § 6809(4)(A) (defining "personally identifiable financial information" as "nonpublic personal information").
172. Mark MacCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 3, 3–6, 11–12 (2011).
173. Cate, *supra* note 21 (noting many and disparate privacy related statutes).
174. *See* Barbara Crutchfield George et al., *U.S. Multinational Employers: Navigating through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 747 (2001).
175. *Id.*

A. Free Speech and Private Information

An often-reiterated rationale for rejecting national data privacy legislation turns on the constitutional protection of free speech.[176] A profound belief in the value of information drives American reluctance to embrace laws that could constrict discourse, knowledge, and exchange of ideas.[177] In fact, some contend that relaxing (or even abolishing) data privacy laws advances privacy interests because open information empowers individuals to access data about themselves and eventually correct false information.[178]

While free speech is expressly protected by the U.S. Constitution, there is no explicit constitutional guarantee of a right to privacy. Many provisions in the Bill of Rights, however, include privacy-related protections. The First Amendment's protections of association and speech, the Third Amendment's prohibition against conscripting private homes to quarter soldiers, the Fourth Amendment's protection against unreasonable searches and seizures, the Fifth Amendment's guard against self-incrimination, and the Fourteenth Amendment's due process and equal protection guarantees all bespeak some aspect of personal privacy.[179]

Regardless, those defending the U.S. approach to data privacy contend that government-mandated restrictions limiting the sharing of personal information, even in the name of "data privacy," violate the First Amendment.[180] The United States and the European Union part ways in the value each assigns to these two conflicting rights. "One person's privacy diminishes another person's right to know, and vice versa,"[181] an oversimplification that nevertheless captures much of the discord underscoring the divergent approaches to data privacy.

Arguments grounded in the First Amendment's protection of free speech are "ascendant in privacy discourse,"[182] and "enjoy[] widespread currency in the legal academy, the private sector, and recent privacy jurisprudence."[183] But they are not unchallenged. Free speech, not infrequently, assumes a larger posture in academic and political debate than the courts historically allow.[184] Free speech protection carries greater significance in civil rights contexts, for example, than in commercial regulation, a distinction that muddies the water and opens the door for attaching greater free speech "rights" than are merited:

176. *See* Huie et al., *supra* note 33, at 402.
177. *Id.*
178. *See* Loring, *supra* note 40.
179. *See* Fred H. Cate, *Privacy and Telecommunications*, 33 WAKE FOREST L. REV. 1, 17–18 (1998).
180. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005).
181. Salbu, *supra* note 85, at 137.
182. Richards, *supra* note 180, at 1149.
183. *Id.* at 1151.
184. *See, e.g.*, *Edenfield v. Fane*, 507 U.S. 761, 765 (1993) ("ambiguities may exist at the margins of the category of commercial speech"); *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 419 (1993) (mentioning the "difficulty of drawing bright lines that will clearly cabin commercial speech in a distinct category"); *Zauderer v. Office of Disciplinary Counsel of the Sup. Ct. of Ohio*, 471 U.S. 626, 637 (1985) (noting that the "precise bounds of the category of . . . commercial speech" are unclear); Samuel A. Terilli, Nike v. Kasky *and the Running-but-Going-Nowhere Commercial Speech Debate*, 10 COMM. L. & POL'Y 383 (2005); Scott Wellikoff, Note, *Mixed Speech: Inequities that Result from an Ambiguous Doctrine*, 19 ST. JOHN'S J. LEGAL COMMENT. 159, 174–79 (2004).

> Such murkiness has allowed what are essentially consumer protection issues in the economic rights context to be transformed into civil rights issues of the highest magnitude, as opponents of data privacy regulation have seized upon the First Amendment as a handy means of derailing proposals to deal with the database problem.[185]

While those who decry adoption of a national data privacy law as violative of free speech have garnered much support, the question is far from resolved.

B. Self-Regulation and Private Information

Another argument made in favor of self-regulation in lieu of a comprehensive data privacy law focuses on the role of government. Historical distrust of centralized power, often projected onto federal government, distinguishes the United States from the European Union. Privacy advocates trumpet national privacy laws as protective of individual civil liberties, but are too often non-conversant in American skepticism of powerful central government. "[W]hen it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart. . . . The European paradigm assumes a much higher comfort level with a far more authoritarian government."[186]

EU data subjects hold a legal right to know what information others have gleaned about them and to know how such information is used.[187] Although such a right is commendable, U.S. businesses customarily process personal information without disclosing anything to their customers. Grocers track consumer purchases via bar code scanners;[188] retailers boost revenue by selling buyer profiles;[189] magazines sell customer lists;[190] photography studios hawk client information;[191] and employers restrict workers' access to their own personnel files.[192] After years of freely processing customer data, requiring businesses to confer notice and obtain consent would seem ludicrous. The market, it is argued, regulates more effectively than centralized government.[193] Market advocates point to the consonance of relaxed data privacy

185. Richards, *supra* note 180, at 1151. *See also id.* at 1149 ("The First Amendment critique . . . mistakenly equates privacy regulation with speech regulation. Building on scholarship examining the boundaries of First Amendment protection, this Article suggests that 'speech restrictions' in a wide variety of commercial contexts have never triggered heightened First Amendment scrutiny, refuting the claim that all information flow regulations fall within the First Amendment.").
186. Jane E. Kirtley, *The EU Data Protection Directive and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 648–49 (1995).
187. *See* Data Protection Directive, *supra* note 58.
188. Christine Anthony, Note, *Grocery Store Frequent Shopper Club Cards: A Window into Your Home*, 4 B.U. J. SCI. & TECH. L. 7 (1998) (warning the public that grocery store membership cards could expose sensitive personal information).
189. Stan Karas, *Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance*, 7 J. TECH. L. & POL'Y 3 (2002).
190. Kramer, *supra* note 48, at 394–95.
191. Dowling, *supra* note 102, at 8.
192. *Id.*
193. P. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 LAW & POL'Y INT'L BUS. 275 (1998). *See also id.* at 288 (stating that the U.S. government also traditionally relies upon the ability of industry to regulate itself, viewing a "complex legal or regulatory infrastructure as an undue restriction on the market"). *But see* Hoofnagle et

law with American expectations.[194] Americans often dismiss the notion that they should be concerned about advertisers' and retailers' use of data.[195]

One study poignantly demonstrates how incessant information harvesting has become entrenched—and therefore expected—among Internet users.[196]

> The absence of a perceptible threat resulted in individuals' reluctance to act to protect their privacy, contributing to the transformation of privacy from an individual right to a public value. As individual users failed to insist on their privacy preferences, the design of Internet architecture was left to the privacy preferences of commercial actors.[197]

Still, advocates of self-regulation maintain that if consumers demanded stricter privacy protections, the market would respond.[198]

C. Private Data as Property

From a legal standpoint, individuals have no property right in their own personal information.[199] U.S. commercial interests balk at recognizing personal information as personal property. Granting property rights in an individual's personal data would arguably promote information privacy in cyberspace by empowering individuals to negotiate with businesses about the uses to which businesses are allowed to process that data.[200] Privacy advocates, unsuccessful and dissatisfied with self-regulation, view attachment of property rights to personal data as a potential solution.[201] "People should own information about themselves, and, as owners of property, should be entitled to control what is done with it."[202]

"Despite 'numerous creative academic proposals for creating property rights in personal information, current case law provides that while individuals have no property rights in their personal information . . . [,] customer information databases are generally viewed as property of the firms that hold them.' "[203] Much has been written on the benefits and detriments of conferring a property right on personal information,[204] which is an academic battle unlikely to materialize in the near term.

---

al., *supra* note 22, at 273 (using empirical study to "invert[] the assumption that privacy interventions are paternalistic while market approaches promote freedom").

194. Preston N. Thomas, Comment, *Little Brother's Big Book: The Case for a Right of Audit in Private Databases*, 18 COMMLAW CONSPECTUS 155, 156 (2009). *But see* Hoofnagle et al., *supra* note 22, at 273.
195. Salbu, *supra* note 85.
196. Gaia Bernstein, *When New Technologies Are Still New: Windows of Opportunity for Privacy Protection*, 51 VILL. L. REV. 921, 922–23 (2006).
197. *Id.* at 924.
198. *See* Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135 (2004).
199. *See* Samuelson, *supra* note 40.
200. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000).
201. *Id.*
202. *Id.*
203. Balaban, *supra* note 125, at 20.
204. *See, e.g.*, Samuelson, *supra* note 40, at 1127; LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, 142–63 (1999) (advocating the use of property rights to protect privacy on the Internet); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383–84, (1996) (arguing that personal information, "like all [other] information,

D. Big Data

U.S. businesses, of course, tend to prefer self-regulation, deferring to non-binding industry codes, and third-party programs for policing themselves and their respective markets. This not only allows business to contain costs by maintaining the status quo, it also fosters the increasingly large data mining[205] and data analytics industry.[206] Capturing information is easy. The difficulty—and potential revenue—comes with the ability to analyze information.[207]

The data aggregation industry is big business in the United States,[208] with data gathering, sorting and selling rapidly becoming the new coin of the kingdom.[209] "Data collection is the dominant activity of commercial websites. Some 92 percent of them collect personal data from web users, which they then aggregate, sort, and use."[210] Data collection—as a source of revenue—was a large industry at the infancy of the EU Directive[211] and continues to grow despite the Directive's wide-ranging reach, which highlights the increasing value of consumer information as a commercial asset.[212] Data analytics was an estimated $25.1 billion industry in 2004[213] and a $105 billion industry in 2010.[214] IBM's 2010 study reveals that eighty-three percent of business leaders identify analytics as a top priority for their businesses.[215] The revenues of the largest data-mining companies exceed $1 billion annually.[216] As one scholar

is property"); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2095 (2004) (suggesting a five-elemental model for personal information as property).

205. Tal Z. Zarsky, *Governmental Data Mining and Its Alternatives*, 116 PENN ST. L. REV. 285, 291 (2011) ("[D]ata mining is defined as the 'nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data.' ").
206. Louie Velocci et al., *Clarity through Data—The Practicality of Forensic Data Mining for Valuators*, J. BUS. VALUATION, Feb. 2009, at 21 ("*Data analytics* is the transformation of data to extract useful information and effectively draw conclusions. This can include the use of statistical modeling, selection of representative subsets of data, curve fitting against an expected outcome, etc. *Data mining*, in contrast, is the application of data modeling, automated computer routines and advanced data sampling techniques aimed at the identification of unforeseen patterns within the data. Data mining uses more complex computer modeling, database analysis and theoretical modeling which often requires a significant investment in software, computer hardware and specialized data analysis resources.").
207. Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Form of Public Opinion*, 5 YALE J.L. & TECH. 1 (2003).
208. Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Policy*, 38 HOUS. L. REV. 717, 719–20 (2001); Paul Rose, Comment, *A Market Response to the European Union Directive on Privacy*, 4 UCLA J. INT'L L. & FOREIGN AFF. 445, 449 (1999).
209. Zarsky, *supra* note 205 (addressing the use of data mining applications in analyzing personal information and its impact upon society).
210. *See* Peppet, *supra* note 29, at 1164 (noting that corporate data mining links at least seven thousand transactions to each individual in the United States per year).
211. Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 775 (1999) ("By 1998, the gross annual revenue of companies selling personal information and profiles, largely without the knowledge or consent of the individuals concerned, was reportedly $1.5 billion.").
212. Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 71–72 (2003).
213. *Id.* at 72.
214. *IBM Sees Biz Analytics Market Growing Sharply*, ECONOMIC TIMES (May 11, 2010), http://articles.economictimes.indiatimes.com/2010-05-11/news/27589148_1_business-analytics-information-integration-ibm-software-group.
215. *Id.*
216. McClurg, *supra* note 212, at 71.

notes, "there is a lot more money (and therefore political clout) behind those companies that want to collect, publish, or use private information."[217] Data processing restrictions, like those embodied by the Directive, threaten those companies that rely, even in part, on data collection and re-use.[218] For companies that do not directly rely on information trafficking for revenue, the cost of compliance with Safe Harbor principles is a disincentive.[219]

Data mining is not limited to private enterprise. The federal government, among other public entities, increasingly employs data mining techniques for law enforcement and other governmental purposes.[220] "Much of the 'privacy' Americans have enjoyed results from the fact that it was simply too expensive or laborious to find out intimate data about them. In the twenty-first century, technology and law have combined to erode the protection for personal privacy previously afforded by practical obscurity."[221] The benefits gained by governmental data mining deter it from advocating on behalf of national data privacy regulation. At bottom, U.S. business interests recognize material costs if European privacy law, which requires fundamental changes in the ease with which marketing data can be garnered, sold, and used, replaces the status quo.[222]

E. Reluctant Conformity

Strong arguments, both ideological and economic, anchor the United States to its sectoral and self-regulatory approach to data privacy regulation. In light of free speech principles, distrust of centralized government, reliance on market-based solutions, and an increasingly profitable data aggregation industry, the United States stands to lose much by adoption of national data privacy law.[223] But the United States is slowly conforming to the EU approach nonetheless. By agreeing to Safe Harbor provisions, has the United States inextricably comingled with European privacy law? Said more dramatically: "I am in blood Stepped in so far that, should I wade no more, Returning were as tedious as go o'er."[224]

More and more U.S. companies are applying for Safe Harbor. The Department of Commerce (DOC) recently announced that approximately fifty companies file initial self-certifications to the Safe Harbor per month.[225] The rate of certification is growing. In a two-year period, 2008–2010, the number of companies joining Safe Harbor certification grew by fifty percent.[226] In 2010, there were more than 2100 companies included on the U.S. DOC's

217. Mark A. Lemley, Comment, *Private Property*, 52 STAN. L. REV. 1545 (2000).
218. Rose, *supra* note 208.
219. *See id.*
220. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 435 (2008).
221. *Id.*; *see also* Kathleen Sullivan, *Under a Watchful Eye: Incursions on Personal Privacy*, *in* THE WAR ON OUR FREEDOMS: CIVIL LIBERTIES IN AN AGE OF TERRORISM 128, 131 (Richard C. Leone & Greg Anrig, Jr., eds., 2003).
222. Salbu, *supra* note 85, at 137.
223. Rose, *supra* note 208.
224. WILLIAM SHAKESPEARE, MACBETH act 3, sc. 4.
225. Brian Hengesbaugh et al., *Why Are More Companies Joining the U.S.-EU Safe Harbor Privacy Framework?*, PRIVACY ADVISOR (Int'l Ass'n of Privacy Prof'ls, Portsmouth, N.H.), Jan.–Feb. 2010, at 1.
226. *See id.*

Safe Harbor list. "Placed in context, this means that more companies join Safe Harbor in a single month than the total number of companies that have obtained approval for binding corporate rules to date . . . ."[227]

Enforcement of data privacy laws has become noticeably more active. The Federal Trade Commission in December 2012 ordered nine data brokerage companies to reveal how they harvest and use data on consumers, toughening the agency's posture toward the multibillion-dollar industry.[228] "The FTC said it plans to use the information it collects to study the industry's privacy practices."[229] In June 2012, a California company agreed to pay $800,000 to settle charges that it illegally sold personal information for employment screening.[230] In December 2010, the FTC released a proposed framework for businesses and policymakers entitled Protecting Consumer Privacy in an Era of Rapid Change.[231] The framework signals the FTC's broadening enforcement scope and increased political will to prosecute data privacy infractions.[232]

Although unsuccessful, several bills have been introduced in Congress that roughly parallel EU data privacy principles. In 1995, Representative Cardiss Collins introduced the Individual Privacy Protection Act of 1995, a bill that would amend the Privacy Provisions of Title and improve individual privacy protections.[233] In just one year, during the term of the 106th Congress, legislators submitted twenty-nine major privacy bills affecting personal data and the Internet.[234] Recently, the Senate Judiciary Committee approved an Act sponsored by Senator Al Franken that requires business to obtain consent from customers before collecting or sharing mobile location data.[235] Debate continues over extensions to the Children's Online Privacy Protection Act (COPPA), and the FTC has prodded Congress to pass a law that would require data brokers to let people examine their personal files culled from their Internet activities.[236]

227. *See id.* at 1.
228. *See* Jessica Guynn, *Federal Trade Commission to Data Brokers: Show Us Your Data*, L.A. TIMES (Dec. 18, 2012), http://www.latimes.com/business/technology/la-fi-tn-federal-trade-commission-to-data-brokers-show-us-your-data-20121217,0,3071455.story.
229. *Id.*
230. Olivera Perkins, *Errors in Background Checks Cost Job Seekers*, CLEVELAND.COM (Dec. 15, 2012), http://www.cleveland.com/business/index.ssf/2012/12/job_applicants_lose_out_as_err_1.html.
231. FEDERAL TRADE COMMISSION (FTC), PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICY MAKERS—PRELIMINARY FTC STAFF REPORT 41 (2011), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
232. *See* Fatima Khan, *Survey of Recent FTC Privacy Developments and Enforcement*, 67 BUS. LAW. 297, 297–303 (2011) (noting the expansion from the FTC's historical enforcement based on either the "notice-and-choice" model or the "harm-based" model to addressing three broader themes: "privacy by design," consumer choice, and transparency of data practices).
233. H.R. 184, 104th Cong. (1995). Representative Collins introduced a substantially similar law in 1991 (H.R. 126, 101st Cong.), and in 1993 (H.R. 135, 103d Cong.). Neither bill passed the initial referral to the House Committee on Government Operations.
234. *Internet Legislation: 106th Congress*, CYBERTELECOM.ORG, http://www.cybertelecom.org/legis/legis106.htm#pri (last visited Apr. 5, 2013).
235. *U.S. Privacy Update*, MRWEB (Dec. 17 2012), http://www.mrweb.com/drno/news16561.htm.
236. *See* Guynn, *supra* note 228.

Breach notification statutes are increasingly popular among state legislatures.[237] At least forty-five states require companies who lose or otherwise fail to secure sensitive data, such as social security and credit card numbers, to inform the affected customers that their personal data has been compromised and possibly pay fines.[238] The increased data privacy regulations in the past two decades,[239] coupled with the surge in companies certifying under Safe Harbor illustrate the pull of the EU Directive, especially in light of the entrenched arguments that militate in favor of self-regulation.

IV. Privacy Law of Tomorrow

The EU Directive is largely viewed as the global standard,[240] as evidenced by the increasing number of countries that continue to adopt national privacy laws consonant with the Directive's proscriptions.[241] The Directive's dominance remains somewhat surprising given its consistent characterization as the strictest data privacy law currently in force.[242] This curiosity is partly explained by the Internet age and by data's borderless nature in conjunction with the Directive's prohibition on data transfers without proof of "adequacy": "either a nation demonstrates to the EU that it can ensure adequate levels of privacy protection, or it loses access to personal data from the EU."[243] By barring data transfers when the transferee lacks the Directive's protections, the Directive effectively offers the transferee (or data processor) a choice: comply with the Directive or risk exclusion from the European market.[244]

Less than five years ago, Canada and Malaysia faced this conundrum. Malaysia, like the United States, has not historically recognized privacy as a fundamental right. Moreover, the Malaysian constitution lists freedom of speech as a fundamental right.[245] Instead of creating a compendium of privacy rights that were industry specific and otherwise self-regulatory like the United States, both Canada and Malaysia enacted national comprehensive data laws that mirror the Directive.[246] They are not alone. "Non-member countries are vying to meet the Directive's 'adequacy' stipulation in order to transact in information arising from EU citizens."[247]

237. Shaw, *supra* note 1161; PRIVACY AND DATA SECURITY LAW DESKBOOK, *supra* note 77, § 15.02.
238. Shaw, *supra* note 161, at 520.
239. Schwartz & Solove, *supra* note 70.
240. *See* Shaffer, *supra* note 59; Joshua S. Bauchner, Note, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, 26 BROOK. J. INT'L L. 689, 705 (2000) (noting Data Directive "de facto extra-territorial effect").
241. Greenleaf, *supra* note 36.
242. Salbu, *supra* note 85, at 137.
243. *Id.* at 140 ("Through the EU's ambitious, wide-reaching strategy, privacy has become the most prominent area of Internet regulation in which one region has tried very aggressively to manage spillover effects by exerting substantial market pressure outside its borders.").
244. *See id.* at 140–41.
245. *See* ELEC. PRIVACY INFO. CTR. (EPIC), PRIVACY AND HUMAN RIGHTS REPORT 2006: MALAYSIA (2006), http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Malaysia.html (noting that Malaysia does not specifically recognize a right to privacy, but does provide a conclusive list of fundamental rights, including freedom of assembly, speech and movement).
246. Yuen, *supra* note 34.
247. *Id.* at 68.

Even so, there are meaningful grounds to reject the Directive. Free speech rights, including a "right to know," and a marketplace of ideas unencumbered by artificial controls as well as a distrust of ceding Internet censorship to government remain robust rationales cutting against the Directive's universal application.[248] Similarly, market-based solutions are arguably more customizable and responsive to consumer demand.[249] Finally, an emerging data aggregation and analytic industry not only offers new income in a down economy, it offers services previously unknown to business.

These benefits inherent in a self-regulatory approach are strengthened when considering the collateral costs attendant to the Directive's reach. When Europe dictates to Canada or Malaysia, for example, what the data privacy law will be in those countries, a disregard for national sovereignty arises that potentially generates political fallout.[250] Certainly both American and European officials chafe at the compromise embodied by Safe Harbor. According to one commentator, the Directive "smacks of imperialism,"[251] evoking questions of whether modern colonialism will be clothed in ones and zeros.[252]

Homogeneity embodies another potential harm. Universal adherence to the Directive creates the norm and threatens an array of approaches that have individualized benefits. Different cultures value different principles. As exemplified by the tension between privacy and free speech, a given nation may value one more than the other. Required compliance with one culture's belief system impoverishes the rest.

A. Emerging Economies

While there is certainly a trend favoring the Directive, full international compliance is by no means inevitable. In Africa, for example, Internet penetration is lower than in the developed world, and Africa's growth rate of Internet users in the last decade has reached 2000%, compared to the global average of 480% growth.[253] Which way will newly wired nations lean? If access to the European market is desired, only one country to date has even made it to the negotiation table, and only then agreeing to a diluted form of compliance with the Directive.

A key for newly data-reliant economies will be bargaining power. Countries seeking access to EU e-commerce and outsourcing markets must, as a preliminary condition, demonstrate "mutually acceptable harmonized regulations that would be a compromise in stringency."[254] So far, only one nation with an international trade portfolio comparable to the EU has successfully forced a meaningful compromise. The fact that only an economic super power has thus far moved Europe off its entrenched position is telling.[255] Even the United States, with

248. Rose, *supra* note 208, at 455–65.
249. *See id.*
250. *See id.*
251. Yuen, *supra* note 34.
252. Cate, *supra* note 220, at 435 ("Today, our biographies are etched in the ones and zeros we leave behind in daily digital transactions." (quoting Sullivan, *supra* note 221, at 131)).
253. *See* Esterhuizen, *supra* note 17; *Africa Internet Use Hits 2,000 Per Cent Growth*, *supra* note 17.
254. David Lazer, *Regulatory Interdependence and International Governance*, 8 J. EUR. PUB. POL'Y 474, 478 (2001).
255. See *id.*

its substantial economic and political clout, negotiated a bypass of the procedures that merely watered down the Directive's requirements. Recall that the core protections required in the Directive are also required for U.S. companies seeking Safe Harbor. The self-certification and U.S. enforcement procedures dilute these requirements, but importantly, the requirements are nearly identical. This highlights the extent of the Directive's international influence on data transfer practices of entities in countries and economies of all sizes.[256] The vital importance of international data transfers enables the European Union to maintain a largely uncompromising stance.

Moreover, what emerging national economy would seek refuge in the U.S. sectoral approach when the international current runs the other way? As of 2011, seventy-six countries have codified national data privacy laws, a consequential number considering that forty years ago there were none.[257] This international trend accelerated shortly after the EU Directive became effective.[258] While a sectoral and self-regulatory approach offers significant benefits, the sheer number of economically significant countries that have signed on represents a powerful dissuader. "For over two decades the rate of adoption of new privacy laws per year has been steadily increasing, and the regions of the globe that have such laws has been steadily expanding."[259] Moreover, countries that have promulgated privacy laws that mirror the Directive tend to be larger in size and economic significance, which further incentivizes emerging countries to join the clear trend.[260]

Without such bargaining power, most countries must comply with the strictest standard in the data protection system.[261] "[T]he cost of failing to actively participate in e-commerce and outsourcing with members of the European Union is more likely to drive firms to organize and lobby their legislators for a political solution that permits cross-border data transfer, than the benefits derived from maintaining the existing data protection regime."[262] Countries will conform to the strictest standards because it is more cost efficient to abide by one regulatory policy—even a strict one—than multiple and divergent versions.[263]

This logic eerily mimics the Directive's twin purposes: (1) protect private data; (2) facilitate free flow of data transfers by requiring a single standard to which all must comply.[264] These goals are seemingly at odds with each other: If Member States legally restrict information traffic in order to protect privacy rights, don't they thereby restrict the free flow of information among Member States? The key to reconciling this apparent conflict is legal uniformity.[265] If the Member States' data protection laws are uniform, no single Member State can

256. Yuen, *supra* note 34.
257. *See* Greenleaf, *supra* note 36.
258. *Id.* abstract (noting that the number and geographical diversity accelerated after 2000).
259. *Id.*
260. *Id.* ("Most other countries that do not yet have data privacy laws are of relatively low significance in international trade, though some countries with large populations are among them . . . .").
261. Lazer, *supra* note 254, at 477–78; Salbu, *supra* note 85, at 137.
262. Yuen, *supra* note 34.
263. Lazer, *supra* note 254.
264. Data Protection Directive, *supra* note 58.
265. *Id.* art. 29. Article 29 establishes the "Working Party" an advisory board made up of representatives from each of the data protection authorities in the various member states. *Id.* The Directive charges

impose differing standards that impede the free flow of information. Binding each Member State to a single standard for processing personal information—even a high standard—promotes privacy protection and facilitates the free flow of information.

V. Conclusion

Thomas Friedman's bestseller, *The World is Flat*, suggested that globalization changed bedrock economic concepts.[266] Historical and geographical boundaries have steadily eroded as information accessibility, international communication, and workflow software facilitate global—rather than national—supply chains. Adaptability and technological intelligence are required for businesses and whole economies to survive in the jaws of inevitable globalization. Friedman posits that the ubiquity of personal computing coupled with fiber optic cable spurred these fundamental shifts in economic function.

This Article suggests that globalization and "flattening" is not limited to economic principles but has bled into international policymaking. The borderless nature of data, when generated or processed on the Internet, is uncoupled from national boundaries and geographical borders. Rulemaking has been historically limited to the sovereign or other political body capable of enforcing the rule, a capability traditionally defined and embodied by nationhood.

> [I]s it open to a State to have resort to its own legal system and, in particular, its own courts for the purpose of making the conduct of foreigners in foreign countries conform to its own commands? . . .
>
> It would seem that the answers to the above questions must be in the negative. Any other result would be repugnant to one's commonsense and the dictates of justice, to that distribution of State jurisdiction and to that idea of international forbearance without which the present international order cannot continue.[267]

The EU Directive ignores that history. It bypasses national sovereignty by prohibiting certain data transfers—heedless of location—if the transfers fail to comply with the Directive.[268] The Directive was never presented as an international treaty nor negotiated as such, and yet it purports to bind entities the world over.[269] "Through the EU's ambitious, wide-reaching strategy, privacy has become the most prominent area of Internet regulation in which one region has tried very aggressively to manage spillover effects by exerting substantial market pressure outside its borders."[270] The United States consistently resists compliance and not without rational justification, but even the world's foremost economic heavyweight has par-

---

the Working Party with fostering a harmonious approach to the implantation of the Directive's requirements. *Id.* art. 30(1).

266. THOMAS FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY (2005).

267. F.A. Mann, *The Doctrine of Jurisdiction in International Law*, 111 RECUEIL DES COURS 145–46 (1964).

268. *See generally*, Kuner, *supra* note 67, at 87; Salbu, *supra* note 85, at 140 ("The global privacy debate is significant for more than the substantive issues it has identified. It also raises critical questions in regard to international relations, as areas or regions try to meet their goals in regard to a technology that has little respect for borders.").

269. Salbu, *supra* note 85, at 140.

270. *Id.*

tially submitted and faces full submission as more and more countries join, leaving the United States increasingly isolated.

"Prior to the explosion of Internet use, a medium through which a state has purported to extend its jurisdiction throughout the entire world has never existed."[271] Undoubtedly, ongoing and serious questions remain as to whether and how the European Union will enforce the Directive as to those entities beyond its legal jurisdiction.[272] As one commentator notes, the question of extraterritorial enforcement may be irrelevant:

> Whatever one's views on this dubious assertion of extraterritorial jurisdiction, the end result for companies is that it pays to ensure that Internet sites served from outside the EU, but could conceivably come within the supervision of EU data protection authorities (e.g., because they collect data from EU residents or otherwise target them), comply with at least the general principles of EU data protection law, or at least that the company running the site has a strategy in place for dealing with inquiries from EU data protection authorities.[273]

The United States faces the prospect of coexisting in the global market with nations whose data-protection schemes are incompatible with the U.S. theme of self-regulation. The increasing importance of international data transfer in the global economy, when combined with a global trend toward comprehensive data protection, highlights the level of success achieved by the European Union in bending international will to conform with it privacy Directive.

271. Moshell, *supra* note 59, at 372.
272. *See* Kuner, *supra* note 67, at 87.
273. *Id.* at 88.