Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law, Cunningham, McKay

McKay Cunningham

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

Follow this and additional works at: http://commons.cu-portland.edu/lawfaculty

Part of the European Law Commons, International Law Commons, Internet Law Commons, and the Privacy Law Commons

CU Commons Citation

PRIVACY IN THE AGE OF THE HACKER: BALANCING GLOBAL PRIVACY AND DATA SECURITY LAW

McKay Cunningham*

Table of Contents

I. INTRODUCTION ........................................ 644

II. THE PRIVACY SIDE .................................... 647
   A. The Information Age .................................. 647
   B. Protecting Private Information .................... 650
      1. Data Privacy Regulation in the European Union ..................................... 651
         a. Initial Attempts to Protect Private Information .......................... 652
         b. The E.U. Directive ........................................ 654
            i. The Directive’s Requirements .................... 655
            ii. The Directive’s Reach ......................... 656
            iii. The Directive’s Reproach ................. 661
            iv. The Directive’s Repercussions ............ 662
         2. Data Privacy Regulation in the United States .................................. 663
            a. The Sectoral Approach ............................... 664
            b. The Safe Harbor .................................. 665

III. THE SECURITY SIDE ................................... 671
   A. The Threat Landscape ................................ 672
      1. Cyberwar ..................................... 673
      2. Consumer Vulnerability ......................... 675
   B. U.S. Response to the Threat Landscape ............ 677
   C. Exceptions for National Security .................. 678

IV. PRIVACY RULES THAT UNDERMINE PRIVACY RIGHTS .... 681
   A. Too Much Privacy is No Privacy At All ............ 682
      1. Protecting Private Data: Evolving Threats .... 684
      2. Protecting Private Data: Evolving Methods ... 687
   B. An Open Window: The European Union’s Proposed Regulation ....................... 690

* Associate Professor, Phoenix School of Law. Member of the Texas Bar. J.D. 2000, Baylor Law School; B.A. 1997, Baylor University. Thanks to Professor Kara Hatfield for her advice and edits.
I. INTRODUCTION

The twin goals of privacy and data security share a fascinating symbiotic relationship—too much of one undermines the other. Unregulated Internet monitoring in security's name emasculates privacy, while privacy laws that heavily burden data sharing and processing corrode data security. Both sides to this inverse relationship suffered a multitude of indignities in 2011.

In November 2011, cyber thieves took $2.7 million from 3,400 Citigroup customers after 360,000 accounts were hacked. Citigroup could not retrieve the data, which included customers' financial data and other personal information. The customers had not misplaced their credit cards or typed out credit card numbers on untrustworthy websites; their only mistake was opening accounts with Citigroup.

Throughout 2011, Saudi Arabia and Israel continued a tit-for-tat school yard scuffle. Instead of trading insults, hackers from the respective nations illegally accessed and published financial and personal information about the other's citizens. A nineteen-year-old Saudi posted online personal information, including financial details of six thousand Israelis. In retaliation, Israeli hackers covertly obtained credit card and other financial details from thousands of Saudis, threatening public disclosure.

In April 2011, Sony suffered a massive breach in its video game online network. Volumes of customer data were compromised,

---


4. Id.

5. Id.
including names, addresses, and possibly credit card data associated with over 77 million user accounts.\textsuperscript{6}

While alarmist sentiment threatens more harm than it hastens help,\textsuperscript{7} the Internet is a rather lawless "place." Cyber threats of almost every ilk are increasing in both frequency and sophistication.\textsuperscript{8} Since 2005, an estimated 543 million records have been lost as a result of more than 2,800 data breaches.\textsuperscript{9} In 2011, data security experts recorded 403 million variants of malware.\textsuperscript{10} "Scholars, government officials, journalists, and computer scientists all agree that inadequate security is an emerging threat—perhaps a catastrophic one . . . ."\textsuperscript{11}

At the same time, logarithmic increases of information—terabytes of data—course through the web, much of it personal and private. At 487 billion gigabytes, if the world's expanding digital content were printed and bound into books it would form a stack that would stretch from Earth to Pluto ten times.\textsuperscript{12} As more people log on and join the digital masses for the first time, data flows inevitably expand, as do calls for protecting private data.\textsuperscript{13} How do we secure data from evolving cyber threats while ensuring that private data is used only by the parties and for the purposes intended?

Where balance is required, unfortunately the international regulatory climate is lopsided. International law tilts unevenly in favor of data privacy. The European Union's Directive 95/46/EC\textsuperscript{14}

\begin{itemize}
  \item \textsuperscript{7} See Karson K. Thompson, Note, \textit{Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate}, 90 Tex. L. Rev. 465 469–71 (2011).
  \item \textsuperscript{10} See Symantec, supra note 8, at 45.
  \item \textsuperscript{11} Derek E. Bambauer, \textit{Conundrum}, 96 Minn. L. Rev. 584, 588 (2011).
  \item \textsuperscript{12} Richard Wray, \textit{Internet Data Heads for 500bn Gigabytes}, Guardian (May 18, 2009), http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion.
  \item \textsuperscript{13} See Tom Silva, \textit{The Era of Big Data Is Here}, HUFFINGTON POST (June 18, 2012), http://www.huffingtonpost.com/tom-silva/the-era-of-big-data-is-he_b_1606914.html (noting that "the aggregate amount of data is growing at 50 percent a year, or more than doubling every two years").
\end{itemize}
(Directive) set the standard for data privacy regulation and facilitated a trend among wired countries toward nationalized data privacy laws. In the less than forty years following the first comprehensive national privacy law (Sweden, 1973), seventy-six countries have followed suit. As Professor Graham Greenleaf notes, "[t]he picture that emerges is that data privacy laws are spreading globally, and their number and geographic diversity accelerating since 2000."16

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. At the current rate of expansion, fifty new laws will emerge in this decade. The most economically significant nations notably absent are the United States, China, and Brazil. India adopted omnibus data privacy laws in 2011, and Brazil is expected to pass such legislation this year, leaving only the United States and China.

By design, omnibus data privacy laws restrict data sharing, a fact that inhibits data security providers who increasingly rely on massive amounts of data to identify and neutralize threats like malware, botnets, distributed denial of service attacks, and Trojan horses. Data privacy regulations rarely include clear exceptions that allow processing of personal data for security purposes. In other words, the bulk of global regulation champions data privacy, often at the expense of data security.

If companies like Citigroup and Sony and countries like Saudi Arabia and Israel cannot safeguard information from incessant hacking, data privacy is somewhat illusory. More than 232.4 million identities were exposed in 2011. Data privacy regulation that refuses the flexibility necessary to process data for security purposes undermines itself.

16. Id.
17. See id.
18. See id.
21. For a discussion of security threats on the Internet, see infra Parts III.A, IV.A.1.
23. See SYMANTEC, supra note 8, at 13.
This Article details the current global regulatory climate in Parts II and III, beginning with a discussion of data privacy regulation before analyzing international responses to data security concerns. In Part IV, the Article argues that one of the gravest threats to data privacy is global data privacy regulation itself. The trend toward more privacy regulation without concomitant security allowances builds privacy walls while ignoring enemies already inside the gate.

II. THE PRIVACY SIDE

A. The Information Age

Ours has been characterized as the age of information. An individual's ability to access and transfer information freely and instantly contrasts readily with previous eras. A market shift from traditional industry to economies based on information manipulation followed computer advances and the digital revolution. Information services and goods constitute the world's largest economic sector. From the emergence of the personal computer in the late 1970s to the burgeoning Internet in the 1990s, information accessibility exploded in mere decades.

Accessibility quickly became dependency. Reliance on information access and the Internet sets the current era apart. The United States is especially dependent. "Every aspect of the U.S. economy and infrastructure depends on digital interconnections." The U.S. Department of Homeland Security reports a high level of integration and reliance:

Our economy and national security are fully dependent upon information technology and the information infrastructure. At
the core of the information infrastructure upon which we depend is the Internet. . . . These computer networks also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace.\(^\text{30}\)

Moreover, critical information infrastructure in the United States is not a segregated silo but rather is owned and operated by diverse government and private entities.\(^\text{31}\) Some say the United States is especially vulnerable to cyber-attacks because so much of the U.S. economy and infrastructure is online, and it is not isolatable or controllable by a single entity.\(^\text{32}\) Increasingly, businesses, schools, news organizations, and financial institutions offer their services exclusively online.\(^\text{33}\)

The Internet age transforms not only business and education but cuts deeper into basic social interactions. Social networking sites continue to increase in popularity and frequency of use, drawing more people online and accounting for more and more of their time.\(^\text{34}\) "The 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."\(^\text{35}\) Younger populations in particular have abandoned traditional forums of social interaction in favor of social networking sites, leaving those without Internet access outside the social norm.\(^\text{36}\)


\(^{32}\) Id.


\(^{36}\) See Teens on Social Networks, eMARKETER (Apr. 16, 2009), http://www.emarketer.com/Article.aspx?R=1007041 (stating that 75% of American teens use social networks and
“Increasingly, being connected to society means being connected to the Internet.”

Dependency on information and the Internet is international; it is not relegated to a few wealthy nations. From 2000 to 2009, the number of Internet users worldwide grew from 394 million to 1.858 billion. China added well over 27 million Internet users in 2011, increasing the total number in China to 485 million. China’s total Internet penetration is at 36.2%—still significantly behind the United States, which is at 77.3%—but the growth rate of new Internet users in China has consistently been in double-digits. In Africa, Internet penetration is lower than in the developed world, but Africa’s growth rate of Internet users in the last decade has reached 2,000%, compared to the global average of 480% growth.

Some countries now deem Internet access a fundamental right. Commentators link the information age to the growth and sustainability of democratic government arguing, for example, that predicting that number to increase to 79% by 2013; see also Memorandum from Amanda Lenhart, Sr. Research Specialist, to Pew Internet & Am. Life Project, Adults and Social Network Websites (Jan. 14, 2009), available at http://www.pewinternet.org/-/media//Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf.pdf (finding that 75% of adults, ages 18–24, use online social networks).


38. See Cate, supra note 27, at 176. See generally Kevin Werbach, Only Connect, 22 BERKELEY TECH. L.J. 1233, 1236 (2007) (stating that “interconnection is the essential input of the new age of abundance”).


41. See id.


"the Internet is, without question, a crucial social and economic pillar of our free and democratic society." The Arab Spring demonstrated both the democratic power and the autocratic threat inherent in the Internet. Insurgents employed a variety of coordination and communication methods dependent on Internet connectivity. Autocrats responded by truncating Internet access altogether, illustrating what others previously thought improbable: that the Internet could be shut down by government.

This trend toward worldwide interconnectedness raises many concerns. An open information system like the Internet, upon which much of the world’s critical infrastructure relies, exposes unique vulnerabilities exploitable by criminal organizations, states, and lone malefactors alike. Because the Internet uses an open architecture, any Internet user is potentially vulnerable.

While cybersecurity and protecting critical infrastructure embody one vulnerability implicit in the information age, protecting private data embodies another. The interplay between cybersecurity and data privacy is complicated and fascinating. The observation at the heart of this Article notes the uneven regulatory climate that promotes data privacy at the expense of cybersecurity. Data privacy regulation is laudable and warranted but given the current threat landscape, it is also vulnerable.

B. Protecting Private Information

Regulating the Internet to protect privacy is no easy task. So far, three salient characteristics attend Internet privacy regulation of any ilk: it is new (and therefore untested); it is trending toward protectionism; and it is not uniform. The contrast between the

47. The regimes in Egypt, Libya, Iran, and Syria largely succeeded, when political crises emerged, in disabling Internet connectivity within their territories. See Kenan, supra note 45.
48. See Bambauer, supra note 11, at 669 (noting that the Internet’s core design both permits open, anonymous communication and allows increased cyber-risks).
49. See id.
50. See LIsA J. SOTTO, PRIVACY AND DATA SECURITY LAW DESKBOOK § 1.04 (2010) ("In light of the global nature of modern information flows, a trend toward global harmonization of data protection principle inevitable. Such harmonization is not imminent, however. With many countries just beginning to enact and enforce their own privacy
United States and the European Union illustrates the disunity most sharply. The European Union has been uncommonly proactive, mandating a privacy directive that not only binds each Member State but also all entities (of whatever nationality) that “process” an E.U. resident’s personally identifiable information.51

It is perhaps this proactive approach that fuels the global trend toward conformity with the E.U. mandate.52 If foreign states and their businesses cannot “process” the personal information of E.U. residents, access to the entire E.U. market is jeopardized. As a result, the E.U. approach to data privacy regulation currently drives worldwide data privacy regulation.53 An understanding of the E.U. policy motivating these regulations is helpful.

1. Data Privacy Regulation in the European Union

In the European Union, privacy is a fundamental right.54 Many attribute the appellation of privacy as a fundamental right to Nazi exploitation of European census records during World War II.55 Nazi review of personal, often classified files resulted in deportation to concentration camps and increased leverage under fascist rule.56 Such abuse in recent history of private and personal information undergirds European vigilance in “protecting personal privacy and resisting state intrusions into private life.”57 Ascribing European privacy vigilance to the Nazis alone, however, is mis-

requirements, this nascent area of the law has not yet matured sufficiently to expect global uniformity.”)

52. Greenleaf, supra note 15, at 11.
The belief that personal information is inseparable from individual autonomy exists beyond the strictures of World War II.  

a. Initial Attempts to Protect Private Information

A few years after World War II, in 1948, the United Nations adopted a Declaration of Human Rights that laid a foundation for establishing legal protection for privacy rights. The Declaration preceded the proliferation of personal information available online and generically provided that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . . ." Several European nations as well as the United States enacted a series of privacy and data protection laws in the following decades. For example, in 1973 the U.S. Department of Health, Education and Welfare provided several protections, including a requirement that any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse. In 1973 and 1974, the Council of Europe's intergovernmental body passed resolutions recommending that member states adopt data protection


59. See id.


61. The U.S. Department of Health, Education & Welfare Code included other protections as well. There must be no personal data record-keeping systems whose very existence is secret; there must be a way for an individual to (a) prevent personal information obtained for one purpose from being used for another purpose without his or her consent, (b) find out what information is in his or her file and how the information is being used, and (c) correct information in his or her records. See U.S. DEP'T OF HEALTH, EDUC. & WELFARE, DHEW PUB. NO. (OS) 73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 124–35 (1973). In 1973, the Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems rejected the creation of a national identifier and advocated the establishment of significant safeguards to protect personal information. See, e.g., id.
laws.\textsuperscript{62} Sweden became the first nation to enact a comprehensive national data privacy law with its Data Act of 1973.\textsuperscript{63}

But it was an international economic organization, rather than a government, that inspired the current European legal framework for data privacy. The Organization for Economic Cooperation and Development (OECD)\textsuperscript{64} laid the foundation in 1980 for future E.U. privacy regulation.\textsuperscript{65} In fact, the divergent privacy laws emerging from European nations frustrated transmission of personal data among them and in part prompted the Council of Europe and OECD to draft guidelines in hopes of unifying data and privacy principles.\textsuperscript{66} Over fifteen years later, OECD guidelines would largely become the backbone of binding legislation throughout each of the E.U. Member States.\textsuperscript{67}

In 1980, however, the OECD guidelines were just that—guidelines. Without binding legal effect, the guidelines failed to harmonize divergent approaches among European nations.\textsuperscript{68} A second attempt the following year by the Council of Europe met the same fate. In 1981, the Council of Europe Convention articulated almost identical guidelines, emphasizing the importance of data and privacy protection, but again failed to unify member nations,

\textsuperscript{62} See Comm. of Ministers, Protection of the Privacy of Individuals Vis-à-Vis Electronic Data Banks in the Private Sector, 224th mtg., Res. (73) 22 (1973); Comm. of Ministers, Protection of the Privacy of Individuals Vis-à-Vis Electronic Data Banks in the Public Sector, 236th mtg., Res. (74) 29 (1974).


\textsuperscript{64} The Organization for Economic Cooperation 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 war-torn Europe. See History, OECD, www.oecd.org/history (last visited Nov. 14, 2012).

\textsuperscript{65} For background information on the OECD, see Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States 136-40 (1999).


\textsuperscript{67} See Kramer, supra note 55, at 398 (citing John Dicke, Internet and Electronic Commerce Law in the European Union 55 (1999)).

\textsuperscript{68} See Cate, supra note 27, at 180; 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, 424 (2002).
who adopted conflicting definitions and interpreted the guidelines inconsistently in their national legislation.  

It wasn't until the fifteen nations comprising the European Community (now the European Union) expanded their goal of a common market to include common polity that a binding and uniform data protection law became possible. 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.” After some revision, the European Parliament approved the draft Directive on March 11, 1992, and the elusive goal of harmonization grew closer with the formal enactment of Council Directive 95/46/EC on October 24, 1995.

b. The E.U. Directive

The Directive's twin purposes are seemingly at odds with each other: (1) protect fundamental privacy rights, and (2) promote the "free flow of personal data between Member States." 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. If the Member States' data protection laws are uniform, no single Member State can 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. It is important to note that despite the European Union's trending unification and despite a Directive that binds Member States, such Directives are only binding with respect to the result to be achieved by Member States. In other words, each Member State retains discretion as to the form

---

70. See Cate, supra note 27, at 181. Although the European Union was formed with the purpose of unifying the national legislation of its Member States, E.U. data protection directives are implemented by Member States under their national laws. See id.
71. 1990 O.J. (C 277) 3.
73. Id.
74. Id. art. 1.
75. 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 the Working Party with fostering a harmonious approach to the implantation of the Directive's requirements. Id. art. 30(1).
and means of implementation.\textsuperscript{76} As a result, privacy and data protection legislation continues to vary somewhat from nation to nation in the European Union.\textsuperscript{77}

i. The Directive’s Requirements

Although each Member State may implement the Directive differently, the Directive provides specific requirements from which Member States draft national legislation.\textsuperscript{78} These requirements are at the core of the global debate on privacy and data security. Personal data must be:

1. Processed fairly and lawfully;
2. Collected for legitimate and specified reasons;
3. Adequate, relevant, and not excessive in relation to the purposes for which it is collected;
4. Accurate and, where necessary, kept up to date; and
5. Retained as identifiable data for no longer than necessary to serve the purposes for which the data were collected.\textsuperscript{79}

While these requirements may appear innocuous, application imposes a heavy burden on many entities that “process” the personal data of E.U. residents. Under these requirements, for example, an E.U. resident has the right to know when personal data is collected.\textsuperscript{80} Entities that collect personal data directly or indirectly must provide such notice. Personal data can only be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.”\textsuperscript{81} Even if collected for a legitimate purpose, an E.U. resident often has the right to choose not to have the personal data collected.\textsuperscript{82} Consent must be a “freely given, specific and informed indication of [the resident’s] wishes.”\textsuperscript{83}

Moreover, a “data subject” (i.e., an E.U. resident whose information is being processed) has the right to know how personal data

\textsuperscript{77} See Sorro, supra note 50, ¶ 1.02[A]; see also id. tbl.18-1 (listing the national data privacy legislation from each individual Member State).
\textsuperscript{78} Data Protection Directive, supra note 14, art. 5 (“Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.”).
\textsuperscript{79} Id. art. 6.
\textsuperscript{80} Id. art. 10. E.U. residents are entitled to know the identity of the data controller, the purposes for which their personal data will be processed, as well as other information regarding fair processing. Id.
\textsuperscript{81} Id. art. 6(1)(b).
\textsuperscript{82} Id. art. 2(h).
\textsuperscript{83} Id.
will be used and to restrict its use. Data collected by an organization must be accurate—individuals have the right to challenge accuracy, mirroring the obligation of data controllers to ensure that inaccurate or incomplete data is corrected. Finally, those who control private data must protect it. Protecting personal data, at minimum, requires that data controllers “implement appropriate technical and organizational measures to protect personal data against . . . destruction or . . . loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network.” Security measures must be “appropriate to the risks represented by the processing and the nature of the data be protected.”

These requirements place immediate and often burdensome obstacles in the path of those who “process” and “control” personal data, or more specifically, “personally identifiable data.”

ii. The Directive’s Reach

Identifying those who must comply with the Directive’s requirements reveals its wide-ranging breadth and reach. Three definitions, all generous in scope, cast a wide net. 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.

It bears repeating that personal data refers not just to names, national identification numbers, social security numbers, and addresses, but includes information that can lead to identification directly or indirectly. Under this “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.” Data is considered personal when it enables anyone to link information to a specific person,

84. Id. art. 6(1)(d).
85. Id. art. 6.
86. Id. art. 17(1).
87. Id.
88. Id. arts. 2, 6, 7.
89. Id. art. 2(a).
90. See id.
91. 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, 1819 (2011) (arguing that infor-
even if the person or entity holding that data cannot make that link. 92

The Data Protection Working Party (Working Party), a representative body from various E.U. Member States charged with fostering consistent interpretation of the Directive’s requirements, issued an opinion in 2007 clarifying the definition of personal information. 93 The opinion broke the definition into component parts: (1) any information; (2) relating to; (3) an identified or identifiable; (4) natural person. 94 The Working Party determined that the third component means a person is identifiable when “although the person has not been identified yet, it is possible to do it.” 95 Thus, information need not identify an individual directly to constitute “personal data,” but the mere fact that the information is related to an individual capable of being identified results in the data being “personal data” under the Directive. 96 “A person may be identified directly by name or indirectly by a telephone number, a car registration number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs.” 97

The Directive couples the broad definition of personal data with a broad definition of data “processing,” defined as:

> [A]ny 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. 98

Any collection, use, and transfer—even the redaction and deletion thereof—constitutes “processing.” 99 This definition purposefully includes data processed automatically as part of a filing system. 100 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

---

92. See id. at 1817.
94. Id. at 6.
95. Id. at 12.
96. Sotto, supra note 50, § 18.02[A].
98. Data Protection Directive, supra note 14, art. 2(b).
99. Id.
100. Id. art. 5, pmbl. ¶ 15.
or any other body which alone or jointly with others determines
the purposes and means of the processing of personal data."101
This definition of data controllers captures more than big busi-
nesses and data aggregators like Epsilon and Axciom. Children
recording orders for Girl Scout cookies, individuals organizing
their business contacts, and students operating websites that
require registration all qualify as data controllers.102

It is tempting to characterize the Directive as affecting Europe
only, as applying to E.U. girl scouts, and those banks, businesses,
and bed and breakfasts between Portugal and Romania. But Article
25, central to the Directive’s international reach, requires that
Member States enact laws prohibiting the transfer of personal data
to non-member states that fail to ensure an “adequate level of pro-
tection.”103 All transfers of personal data to countries outside the
European Union are prohibited where the legal regime in that
country does not meet an adequate level of privacy protection.104

The Directive provides that the adequacy of the protection
offered by the transferee country “shall be assessed in the light of
all 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 mea-
sures which are complied with” in that country.105 The European
Council regards only nine countries as “adequate.”106

A handful of alternative approaches allow individuals and orga-
nizations that are not citizens of these nine countries to process

---

101. Id. art. 2(d).
102. See Cate, supra note 27, at 183.
104. Id.
105. 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. Id. art. 25(2). The prohibition in Article 25 is subject to
exemptions, provided in Article 26, when (1) the data subject has consented “unambigu-
ously” 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.
E.U. personal data. These approaches are discussed more fully below, and have the effect of applying the Directive’s prescriptions to the individual or organization rather than their home nation.

In the age of information, data flows do not stop at the border. The exact origin of any given data, or the nations, if any, associated with that data may be impossible or impracticable to discern. In other words, the impracticability of separating data collected or derived from E.U. Member States requires multinational businesses to conform their entire data processing policies to the Directive’s mandate. Just because a business does not reside or physically operate in Europe does not immunize it from complying with the Directive, if that business uses, transfers, automates, or collects personal data about E.U. residents.

To give perspective, companies with 1,000 employees or more harbor on average 235 terabytes of data—more information than is housed in the Library of Congress. The probability is high that those 235 terabytes will include E.U. personal data of some sort, especially given the broad definition of “personal data.” The flattening of the world economy accounts in large part for the worldwide trend of conforming to the European Union’s data privacy law. The broad reach of the Directive not only affects businesses and individuals operating outside the European Union, it also encumbers E.U. organizations that transfer data to non-E.U. organizations. In such cases, the compliance framework might function as follows:

First, an E.U. data controller must comply with a national data protection law, which was enacted pursuant to the Directive. At minimum, the law requires notification to the local Data Protection Authority (DPA) and to individual data subjects, restriction of data use to the ends specified and necessary, minimization of data

---

107. See infra Part II.B.1.iv.
108. See Cate, supra note 27, at 179 (“Information, especially digital information, is inherently global. Data ignores national and provincial borders, and, unlike a truckload of steel or a freight train of coal, data is difficult to pinpoint and almost impossible to block, through either legal or technological means.”).
111. Silva, supra note 13.
112. See Shaffer, supra note 109, at 22–38.
113. See Leathers, supra note 110, at 198–200.
retention, implementation of data security measures, and appointment of a data protection officer within the organization. Of course, these requirements apply notwithstanding transfer to a non-E.U. organization.

Second, the E.U. organization must vet the non-E.U. organization (data transferee) to ensure that the transferee provides adequate data protection. More often than not, the transferee must agree to contractual obligations binding it to act according to the E.U. data controller’s instructions. Again, this requirement would also attend data transfers wholly within the European Union.

Finally, the E.U. organization must ensure the transferee adequately complies with the Directive. There are a number of ways to ensure such adequacy: (1) the European Council formally recognizes the transferee’s nation as having and enforcing laws that essentially mirror the Directive; (2) the transferee agrees to certain model clauses that mirror the Directive’s requirements; (3) the transferee adopts binding corporate rules that mirror the Directive’s requirements; or (4) the transferee has self-certified itself as substantially complying with the Directive’s requirements as a safe harbor.

These hurdles are not easily met. They also depend on whether a given party to a data transfer is a data controller or data processor. The Directive distinguishes between data controllers and data processors, providing that a data processor is any entity that processes personal data on behalf of the controller. Although this distinction may appear simple, the line marking where a controller ends and a processor begins blurs easily and often in the world of free flow information. If a service provider contractually reserves or exercises too much control over relevant data, it

---

114. See Sotto, supra note 50, § 1.02[A]; see also id. tbl. 18-1 (listing the national data privacy legislation from each individual Member State).
115. See id.
116. See Mark Jeffery, Information Technology and Workers’ Privacy: The English Law, 23 COMP. LAB. L. & POL’Y J. 301, 319–21 (2002) (“Data Controllers retain an important degree of responsibility for the actions of the Data Processor. The Data Protection Act requires them to choose a Data Processor who takes measures to guarantee the security of the personal data and to ensure that the Data Processor puts these measures into practice.”).
117. Id. at 320.
118. Id.
120. Id. art. 2(e).
becomes a data controller.\textsuperscript{122} Many large companies are affiliated with others or have subsidiaries exercising various degrees of independence. In other contexts, contractual clauses self-identify an entity as a data processor while simultaneously reserving control over data.\textsuperscript{123} And in still other circumstances multilayered sub-contracting blends controller with processor.\textsuperscript{124} The distinction is important because data controllers shoulder greater obligations and face liability and fines under the Directive.\textsuperscript{125}

\textit{iii. The Directive's Reproach}

E.U. Member States are required to enact dissuasive civil penalties or other liability for data controllers that unlawfully process personal information.\textsuperscript{126} Both government officials and data subjects may initiate proceedings, creating a "right of every person to a judicial remedy for any breach of the rights guaranteed by this Directive."\textsuperscript{127}

Enforcement differs from Member State to Member State, but generally noncompliance results in fines, public reprimands, and/or possible imprisonment for criminal offenses.\textsuperscript{128} Perhaps the most publicized criminal case erupted when an Italian judge convicted three Google executives on charges of failure to exercise control over personal data.\textsuperscript{129} An Internet user had uploaded a three-minute video to Google Video featuring school kids insulting and berating an autistic boy named Francesco Giovanni De Leon in Turin, Italy.\textsuperscript{130} The video garnered over five thousand viewings in the two months that followed its posting as well as at least one plea for Google to remove it.\textsuperscript{131} The video was not removed until Italian officials demanded removal, sparking a criminal investiga-

\footnotesize{\begin{itemize}
\item \textsuperscript{122} See 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, 979 (2006).
\item \textsuperscript{123} See Francoise Gilbert, Privacy & Security Report: Cloud Service Providers Can Be Both Data Processors and Data Controllers, 10 Privacy & Sec. L. Rep. (BNA) 791 (Feb. 14, 2011).
\item \textsuperscript{125} Data Protection Directive, \textit{supra} note 14, art. 17.
\item \textsuperscript{126} \textit{Id.} arts. 22-24.
\item \textsuperscript{127} \textit{Id.}
\item \textsuperscript{128} \textit{Id.} pmbl. ¶ 63.
\item \textsuperscript{130} See Hampson, \textit{supra} note 129, 479–80.
\item \textsuperscript{131} \textit{Id.}
\end{itemize}}
tion that that ended in the convictions of three Google executives, principally for violation of Italy’s Personal Data Protection Code.\textsuperscript{132} One privacy group described it as the first criminal sanction ever pursued against a privacy professional for his company’s actions.\textsuperscript{133}

A Member State’s DPA may investigate potential infractions of its national data protection law either on receipt of an individual’s complaint or on its own suspicion of a violation.\textsuperscript{134} Some DPAs have authority to audit a controller’s files without third party permission or a court order.\textsuperscript{135} In 1999, a Belgian court fined Yahoo! Inc. $55,000 for failing to disclose its email user’s personal data to the Belgian prosecutor.\textsuperscript{136} In most Member States, failure to register data processing activities with the DPA is a criminal offense.\textsuperscript{137}

d. The Directive’s Repercussions

Articles 25 and 26 of the Directive are particularly relevant to electronic commerce because they require all nations with whom Member States conduct business to subject themselves to the Directive’s scrutiny, barring transfers to any country lacking an “adequate” level of protection.\textsuperscript{138} It is this far-reaching aspect of the E.U. Directive that largely pressures non-E.U. nations to adopt omnibus legislation that mirrors the Directive’s data privacy requirements.\textsuperscript{139}

As mentioned above, there are four principle mechanisms by which non-E.U. organizations may lawfully process personal data under the E.U. Directive: (1) an “adequacy” determination, (2) compliance with safe harbor provisions, (3) adoption of model contracts;\textsuperscript{140} or (4) adoption of binding corporate rules.\textsuperscript{141} An adequacy determination reflects the European Commission’s (the Commission) formal recognition that a non-E.U. country has

\begin{itemize}
  \item \textsuperscript{132} See id.
  \item \textsuperscript{133} See Criminal Trial Against Google Exes to Resume, INT’L ASS’N PRIVACY PROFS. (Mar. 1, 2009), https://www.privacyassociation.org/publications/2009_03_criminal_trial_against_google_execs_to_resume/.
  \item \textsuperscript{134} Data Protection Directive, supra note 14, pmbl. ¶ 63.
  \item \textsuperscript{135} See SOTTO, supra note 50, § 18.02 n.189 (noting that Data Protection Authorities in France and Netherlands have auditing authority).
  \item \textsuperscript{136} Id.
  \item \textsuperscript{137} Id. (noting Belgium, France, Greece, Norway, and the United Kingdom as examples).
  \item \textsuperscript{139} Moshell, supra note 58, at 364 (suggesting that the “most significant rationale is the desire to ensure that a nation’s laws are consistent with the European model”).
  \item \textsuperscript{140} See generally Determann, supra note 121, at 510.
  \item \textsuperscript{141} Data Protection Directive, supra note 14.
\end{itemize}
enacted legislation or has otherwise demonstrated an adequate level of protection for personal data.\textsuperscript{142} As noted above, only nine countries have satisfied the Commission’s adequacy review: Andorra, Argentina, Canada, Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, and Switzerland.\textsuperscript{143}

While nine countries may not sound like much, achieving an “adequacy” rating from the Commission is not the only compliance mechanism. Many nations are conforming to the Directive’s requirements through national legislation. In fact, some nations’ constitutions ensure the right to privacy in some manner, with more recent iterations including “specific rights to access and control of one’s personal information.”\textsuperscript{144} An increasing number of non-E.U. nations have enacted or are in the process of enacting omnibus data protection laws.\textsuperscript{145} In two decades, 1990 to 2010, fifty-one national data privacy laws emerged, many directly patterned after the E.U. Directive. Of the world’s largest economic nations, notably absent from this trend are the United States, China, and Brazil (which is expected to pass legislation this year).\textsuperscript{146} The majority of the new omnibus legislative regimes apply broadly to any person or entity that processes personal information and differ markedly from the fragmented data privacy laws in the United States.

2. Data Privacy Regulation in the United States

The United States is conspicuously resolved and increasingly isolated in its refusal to pass comprehensive data privacy legislation. Unlike in Europe, U.S. law does not recognize an absolute right to privacy.\textsuperscript{147} The U.S. Constitution does not explicitly protect privacy, but privacy protections have been found in certain instances deriving from the First, Fourth, and Fifth Amendments.\textsuperscript{148} The Third and Fourteenth Amendments have also given rise to privacy

\textsuperscript{142} See id. pmbl. ¶ 57, art. 25(1).
\textsuperscript{143} See Greenleaf, supra note 15, at 11-17.
\textsuperscript{144} See Moshell, supra note 58, at 364.
\textsuperscript{146} See Monteiro, supra note 20.
\textsuperscript{147} See ALAN F. WESTIN, PRIVACY AND FREEDOM 25 (1970) (noting that the right to privacy is not absolute); Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 214-18 (1890) (suggesting when the right to privacy must yield to public welfare).
related protections. This Constitutional patchwork parallels the legislative “sectoral” approach to data privacy in the United States.

a. The Sectoral Approach

Of course, the United States is not without privacy regulation, but the laws protecting data and information privacy have been widely characterized as “sectoral,” a reference to fragmented and industry-specific regulation. The industries constrained by data protection legislation are those that traditionally handle sensitive private data, and the laws are often narrowly tailored, addressing particular elements of personal information or discrete uses of discrete data. U.S. regulation is further complicated by state and local data privacy regulation. For example, the federal Health Insurance Portability and Accountability Act does not have preemptive effect, leaving state governments room to create further legislation affecting medical and health information.

Other examples of the U.S. sectoral approach include the Telecommunications Act of 1996, which restricts telecommunications carriers’ use of private customer information; the Gramm-Leach-Bliley Act, which restricts financial institutions’ use and dissemination of private financial data; and the Fair and Accurate Credit Transactions Act, which restricts credit reporting and increases protections for related personal information.

Use of consumer information collected for entertainment subscriptions provides an apt illustration of fragmented regulation in the United States. Three separate statutes regulate use of name and address information depending on whether the subscription is for cable television, telephone service, or video rental. Whereas the European Directive states a single definition of per-
sonal data governing its twenty-seven Member States, the U.S. sectoral approach spawns multiple, often disparate, definitions. The definition of personal data under the Fair Credit Reporting Act, for example, differs from the Video Privacy Protection Act, which differs from the Gramm-Leach-Bliley Act.

This disjointed and industry-specific regulation of data privacy has prompted calls for omnibus federal privacy legislation. While comprehensive legislation overriding the patchwork of federal and state legislation would certainly lend harmony, most commentators agree that such an approach is unlikely in the near term.

Unsurprisingly, this conglomeration of varied privacy protections does not satisfy the mandated requirements that govern E.U. Member States. E.U. officials had hoped to sway U.S. lawmakers to enact a comprehensive privacy regime, but basic differences in the role of government and fundamental rights have thus far prohibited it.

b. The Safe Harbor

In light of the above disparities, how do U.S. organizations conduct business within E.U. Member States? If the E.U. Directive restricts transfers of E.U. residents’ personal information, and if the definition of “personal information” is extremely broad, are Amazon, Facebook, Google and a multitude of other U.S. businesses barred from the European market?

Of course it is not just Amazon, Facebook, and Google that are affected; the “inadequacy” of U.S. data protection laws threatens a

160. See Data Protection Directive, supra note 14, art. 2.
161. 15 U.S.C. § 1681(b) (2006) (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).
164. Recent reports by the Department of Commerce and the Federal Trade Commission on online privacy indicate that both agencies plan to play significant roles in this area. See, e.g., DEP’T OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010); FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010).
165. See, e.g., Sotto, supra note 50, § 1.04 (noting that “harmonization is not imminent”).
host of interactions, including airline reservations, on-line purchases, tens of millions of emails, transatlantic banking, to say nothing of the more than nine million European employees of American companies whose personal information would be inaccessible. As one scholar has noted, such a policy "would immediately destroy a $1.5 trillion transatlantic economic relationship."  

To avoid such a fate, the U.S. Department of Commerce and the European Commission negotiated for two years before agreeing to a "Safe Harbor" exception in 2000 that allows continued business between the trading partners. The compromise sought to bridge the differing approaches in the European Union and the United States, streamline the means for U.S. organizations to comply with the E.U. Directive, and protect E.U. organizations that transfer personal data to U.S. organizations. Eligibility for Safe Harbor protections requires U.S. organizations to be subject to jurisdiction of the Federal Trade Commission (FTC) or Department of Transportation. The Safe Harbor requirements themselves largely track the E.U. Directive's requirements, although not precisely.

The Safe Harbor principles are:

1. Notice: When their personal data is processed in the United States, E.U. citizens must be given notice of (1) the purposes for which their personal information is collected and used, (2) the types of third parties to whom their data are disclosed, (3) the certifying organization's contact information for possible complaints, and (4) the choices

167. See Cate, supra note 27, at 194–95.
169. See Safe Harbor, supra note 168.
available to limit the use and disclosure of their personal
data.
2. Choice: E.U. citizens must have the opportunity to opt out
of having their personal data disclosed to third parties or
used for a purpose incompatible with that for which the
data was originally collected. Opt-in consent is required for
disclosures of "sensitive" personal data.
3. Access: E.U. citizens must have access to their data to
ensure its accuracy.
4. Security: The U.S. organization must take reasonable steps
to protect the personal data from loss, misuse, and unau-
thorized access, disclosure, and destruction.
5. Data Integrity: The U.S. organization must ensure the data
are relevant and reliable for their intended purposes.
6. Enforcement: The U.S. organization must provide effective
enforcement mechanisms to facilitate complaints and
disputes.

If the requirements above largely mirror those of the E.U. Direc-
tive, where is the compromise? Are U.S. organizations essentially
complying with the Directive? There are many subtle differences
between the two regimes that are not insignificant, but the most
notable is that use of Safe Harbor is voluntary, self-certifying, and
largely unenforced. U.S. businesses that process E.U. personal
data have been described as self-regulating. Companies that
apply for Safe Harbor self-certify. In other words, no government
official reviews and then authorizes whether any given company in
fact complies with Safe Harbor principles before awarding certifi-
cation. A company need only notify the U.S. Department of Com-
merce that it intends to comply with Safe Harbor and publicly
declare compliance on its website.

In practice, a U.S. organization that self-certifies through Safe
Harbor is then afforded automatic approval from data processing
authorities in the European Union. Moreover, Safe Harbor certi-

172. See U.S.-E.U. Safe Harbor Overview, supra note 170; Sotto, supra note 50, § 18.02.
173. See Zaidi, supra note 171, at 176.
174. See Leathers, supra note 110, at 196. The Safe Harbor agreement is followed by
entities on a voluntary basis. See Zaidi, supra note 171, at 176. Alternatively, a company
may develop its own self-regulatory policies, notify the Department of Commerce (DOC)
and publicly declare its compliance. See Angela Vitale, The EU Privacy Directive and the Regu-
lating Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet, 35
VAND. J. TRANSNAT'L L. 321, 339 (2002). Finally, voluntary compliance may be achieved
through complying with a "safety seal" program that notifies the DOC of the company's
participation and ensures compliance.
175. See Sotto, supra note 50, § 18.02[B].

Citation shifts the jurisdiction over transfers from E.U. authorities to the U.S. Department of Commerce and the FTC.\(^\text{176}\) The FTC enforces the Safe Harbor requirements pursuant to section five of the Federal Trade Commission Act, which generally proscribes “unfair or deceptive acts or practices in or affecting commerce.”\(^\text{177}\)


Some commentators contend that the American approach to privacy protection is driven by business interests, as compared to the E.U. rights-based approach.\(^\text{178}\) The data aggregation industry—which performs data gathering, sorting, and selling—is big business in the United States.\(^\text{179}\) One scholar has noted that: “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.”\(^\text{180}\) Data collection—as a source of revenue—was a large industry at the infancy of the E.U. Directive\(^\text{181}\) and continues to grow despite the Directive’s wide-ranging reach, which highlights the increasing value of consumer information as a commercial asset.\(^\text{182}\) Data analytics was an estimated $25.1 billion industry in 2004\(^\text{183}\) and a $105 billion industry in 2010.\(^\text{184}\) A 2010 study by IBM reveals that 83% of business leaders identify analytics as a top priority for their businesses.\(^\text{185}\) The revenues of the largest data-mining companies exceed $1 billion annually.\(^\text{186}\)

\(^{176}\) See id.


\(^{178}\) See, e.g., Bignami, supra note 56.


\(^{181}\) Reidenberg, E-commerce, supra note 179, at 775 (“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.”).


\(^{183}\) Id. at 72.


\(^{185}\) See id.

\(^{186}\) McClurg, supra note 182, at 71.
Data processing restrictions, like those embodied by the Directive, threaten those companies that rely, even in part, on data collection and re-use. For companies that do not directly rely on information trafficking for revenue, the cost of compliance with Safe Harbor principles is a disincentive. Certification under the Safe Harbor subjects a given company to FTC jurisdiction and opens potential liability stemming from E.U. residents and Member States. Similarly, the cost of restructuring a company's information processes to provide end users notice, access, and rights of refusal can be substantial.

Finally, lackluster enforcement allows companies to give lip service to data privacy without full compliance. The voluntary and self-regulating scheme applicable in the United States reflects the philosophy that the "marketplace will protect privacy because the fair treatment of personal information is valuable to consumers," a notion that rankles E.U. policymakers who insist on direct governmental oversight and implementation. E.U. officials point to the fact that it took the FTC nine years to bring its first data privacy enforcement action against a U.S. company that falsely professed to comply with Safe Harbor principles.

In short, 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. Those that arguably comply with Safe Harbor rules make up only a portion of U.S. companies that would suffer "severe, adverse effects" if data transfers from the European Union were blocked. As of October 2006, approximately 1,000 companies were participating in the program, 190 of which were "not current" in their certifica-

189. See Leathers, supra note 110, at 195–96.
190. 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."); see also Press 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.
191. Barnes, supra note 171, at 181.
tion.\textsuperscript{192} Although the number of self-certifying organizations increased since 2006,\textsuperscript{193} questions remain whether the number will continue to grow and whether those that have self-certified in fact comply.\textsuperscript{194}

Unsurprisingly, E.U. policymakers are unsatisfied with U.S. efforts. Even before officials agreed to Safe Harbor principles, privacy advocates and E.U. officials levied heavy criticism at what they saw as a diluted version of the Directive.\textsuperscript{195} Two years into the Safe Harbor agreement, an E.U. Commission issued a working paper tracking the implementation of Safe Harbor principles in the United States.\textsuperscript{196} The Commission found that a significant number of companies failed to observe “the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies.”\textsuperscript{197} The Commission determined that U.S. companies often fail to even display the mandatory public statement of adherence to the Safe Harbor principles.\textsuperscript{198} Many of the privacy statements that the Commission did locate inaccurately reflected Safe Harbor principles, leading the Commission to conclude that “less than half of organizations post privacy policies that reflect all seven Safe Harbor Principles.”\textsuperscript{199} According to an independent FTC survey, only 20\% of websites that collect personal identifying information implement all of the fair information practice principles.\textsuperscript{200}

\textsuperscript{192} Id. at 181–82.

\textsuperscript{193} For the current list, see \textit{U.S.-EU Safe Harbor List}, EXPORT.GOV, http://safeharbor.export.gov/list.aspx (last visited Nov. 14, 2012); see also Brian Hengesbaugh et al., \textit{Why Are More Companies Joining the U.S.-EU Safe Harbor Privacy Framework?}, PRIVACY ADVISOR, Jan.–Feb. 2010, at 1, 1 (noting that 2,100 companies were listed on the U.S. Safe Harbor list as of 2009).

\textsuperscript{194} See Nijhawan, supra note 188, at 945 (noting that U.S. businesses see self-certification as creating more problems than not joining).


\textsuperscript{197} Id. at 2.

\textsuperscript{198} Id. at 8.

\textsuperscript{199} Id.

\textsuperscript{200} See Prepared Statement, Fed. Trade Comm'n, Privacy Online: Fair Information Practices In the Electronic Marketplace, Before the Committee on Commerce, Science,
Slow incremental change, if any at all, will mark the current decade's battle between those who favor the U.S. sectoral and market-friendly approach to privacy protection legislation and those who advocate for comprehensive E.U.-like legislation. Plenty of voices color both sides of the debate. Many privacy advocates look to the Directive as the template to which all companies should conform their privacy practices. Others argue that the current U.S. market-based approach is unfair and provides insufficient consumer protection, while still others resist the European Union's top-down, government-imposed methodology to data privacy regulation.

These competing voices analyze which approach best protects data privacy, but data privacy is only half of the equation. Dramatically absent from the above debate is a clarion call for data security and attendant legislation facilitating the same. Data privacy and data security are interlinked, yet the current discourse relegates data security to a secondary concern. Favoring privacy over security is more puzzling still given the acceleration of cyber-attacks against countries, Fortune 500 businesses, and individuals.

III. The Security Side

Data privacy regulation on a global scale continues to accelerate. Even the United States, while lacking comprehensive legislation, has increased data privacy regulations in the past two decades. Protecting personal, and often sensitive, information is certainly laudable, but global regulation appears to lean unevenly toward protectionism without concomitant flexibility for data


201. But see Shaffer, supra note 109, at 22–38 (predicting that U.S. privacy standards would converge with European standards).


203. Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 BERKELEY TECH. L.J. 771, 787 (1999); Reidenberg, E-commerce, supra note 179, at 726 ("[R]eliance on self-regulation is not an appropriate mechanism to achieve the protection of basic political rights. Self-regulation in the U.S. reduces privacy protection to an uncertain regime of notice and choice."); see also Shaffer, supra note 109, at 64.

204. See Nijhawan, supra note 188, at 975–76.


207. See Schwartz & Solove, supra note 91, at 1819.
security. This Article argues for placing such flexibility in the hands of individuals and private organizations, but without increasing national or governmental authority to censor or control data flows. In the United States, for example, the Patriot Act and proposed “kill-switch” laws concentrate too much power in national government. The E.U. Directive exempts national governments from adhering to its strictures when governments process personal information for national security purposes, but the Directive leaves little legal footing for non-governmental entities to do the same.

A study of the threat landscape, below, reveals an Internet saturated by hacking, cybercrime, and cyberwar. “Scholars, government officials, journalists, and computer scientists all agree that inadequate security is an emerging threat – perhaps a catastrophic one . . . .” Regulatory response to these threats both in the United States and in Europe demonstrate a disproportionate reliance on government to provide security, with little encouragement or provision for security in the private sector.

A. The Threat Landscape

The chief cyber official at the Federal Bureau of Investigation (FBI) spoke about cyber threats late in 2011 at the Conference on Cyber Security in New York. He confirmed the increased frequency and severity of online crime and illegal hacking, noting that American companies and consumers fail to realize the seriousness and magnitude of cyber threats. The risk to business was deemed “existential, meaning it could eliminate whole companies.”

---

208. See Bambauer, supra note 11, at 587 (identifying that the “current failure to meaningfully address this problem occurs because cybersecurity is undertheorized”).


210. See Data Protection Directive, supra note 14, art. 3(2).

211. Bambauer, supra note 11, at 588.

212. See, e.g., Data Protection Directive, supra note 14, art. 3(2) (exempting national governments from data privacy regulation when processing data for security purposes). No such exemption is provided for non-government security.


214. Gerry Smith, Cyber-Crimes Pose ‘Existential’ Threat, FBI Warns, HUFFINGTON POST (Jan. 12, 2012), http://www.huffingtonpost.com/2012/01/12/cyber-threats_n_1202026.html (“We’ve seen the number and sophistication of the attacks by these cyber actors increase dramatically.”).

215. Id.
By way of illustration, the official recounted several recent FBI investigations. In one, hackers drove a company out of business after stealing $5 million from its accounts.\textsuperscript{216} In another, hackers took a decade of research estimated to be worth $1 billion "virtually overnight."\textsuperscript{217} And in another, hackers gained access to health services records, encrypted the records, and demanded money before decrypting the records.\textsuperscript{218} "Hundreds of millions of dollars have been stolen, primarily through the financial services sector, just in the last couple years."\textsuperscript{219}

During 2011, conventionally termed the "Year of the Hacker,"\textsuperscript{220} major organizations including Sony,\textsuperscript{221} the U.S. Chamber of Commerce,\textsuperscript{222} Google,\textsuperscript{223} and Amazon\textsuperscript{224} revealed that hackers had penetrated their networks to steal corporate secrets or leak sensitive customer data.\textsuperscript{225}

Hacking isn't limited to stealing from commercial enterprises. President Obama characterized cyber threats as "one of the most serious economic and national security challenges we face," positing that "America's economic prosperity in the twenty-first century will depend on cybersecurity."\textsuperscript{226}

1. Cyberwar

"Cyberwar," a word laden with connotation, will soon be common parlance in our lexicon.\textsuperscript{227} Although the term is elusive to

\begin{thebibliography}{10}
\bibitem{216} Id.
\bibitem{217} Id.
\bibitem{218} Id.
\bibitem{219} Id.
\bibitem{224} Peter T. Leeson, \textit{The Economics of Computer Hacking}, 1 J.L. Econ. & Pol'y 511, 514 (2005).
\bibitem{225} See generally \textsc{Symantec}, supra note 8.
define, Richard Clarke in his book *Cyber War* defines cyberwar as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”\(^{228}\) Such actions are increasingly common.

For example, Estonia’s entire nationwide network collapsed in 2007.\(^{229}\) Even though it is one of the most wired nations on the globe, Estonia’s national network shut down after politically-motivated hackers forced a data load equivalent to downloading the entire Windows XP operating system every six seconds for ten hours.\(^{230}\) Estonia’s largest bank lost around $1 million over the course of the attacks, and Estonia’s parliament members could not access email for four days.\(^{231}\)

Saudi Arabia and Israel have waged an ongoing hacking battle. Hackers identifying themselves as Group XP claimed to have gained access to 400,000 Israeli credit card accounts.\(^{232}\) A nineteen-year-old Saudi national later posted online credit card details of 6,000 Israelis and other personal information, noting that he had access to tens of thousands more.\(^{233}\) In retaliation, the Associated Press reports that Israeli hackers obtained credit card and bank details from thousands of Saudi citizens and threatened to release them publicly.\(^{234}\)

One of the more famous politically-motivated cyber-attacks targeted Iran. That attack, allegedly perpetrated by the United States and/or Israel, involved the Stuxnet worm, which was said to be the most sophisticated malware yet discovered and purpor-

---

\(^{228}\) Richard A. Clarke, *Cyber War* 33 (2010).


\(^{231}\) Id.


\(^{233}\) Id.

tedly destroyed one thousand centrifuges used for uranium enrichment.235

2. Consumer Vulnerability

Hacking and cyber-attacks affect nations and individuals alike.236 As the Internet user base grows, more critical information appears online and a corresponding increase of hacking emerges. Ten years ago, an average American’s information could be found in anywhere between twenty-five and one hundred commercial databases,237 a number that is certain to be much larger today. In 2011, more than 232.4 million identities were exposed.238 A Price-waterhouse Coopers survey—from ten years ago—reported that 78% of U.S. companies responding had suffered at least one network security breach.239 A 2011 security threat report notes that cyber-attacks are not limited to large businesses, citing an increase in targeted attacks against smaller organizations.240 The report indicates that such data “could represent a trend in attackers focusing their attention on lower hanging fruit.”241

Cyber-crime is prolific, in part, because it is difficult to police. Perpetrators enjoy a certain level of anonymity.242 Detection and


236. See Smith, supra note 214 (noting that Federal Bureau of Investigation officials categorized the largest modern hacking threats into three profiles: (1) nations targeting research and development and corporate secrets and strategies; (2) terrorists targeting critical infrastructure; and (3) organized criminals out for profit).


238. See Symantec, supra note 8, at 13.

239. See Mary M. Calkins, Note, They Shoot Trojan Horses, Don’t They? An Economic Analysis of Anti-Hacking Regulatory Models, 89 Geo. L.J. 171, 173 (2000) (citing Amy K. Larsen, Global Security Survey: Virus Attack, InformationWeek (July 12, 1999), http://www.informationweek.com/743/security.htm). These results are even more potent given that the great majority of hacking incidents go unreported. See id. at 183. The target of an attack may fail to detect intrusion, or more often, the target chooses not to report. Id. Businesses do not want bad publicity. See id. Also, reporting a successful intrusion announces vulnerability and encourages copycats. Id.; Ian C. Ballon, Alternative Corporate Responses to Internet Data Theft, in 17TH ANNUAL INSTITUTE ON COMPUTER LAW: THE EVOLVING LAW ON THE INTERNET—COMMERCE, FREE SPEECH, SECURITY, OBSCENITY, AND ENTERTAINMENT (1997).

240. See Symantec, supra note 8, at 12 (stating that “50% of attacks focused on companies with less than 2500 employees, and 18% of attacks were focused on organizations with less than 250 employees”).

241. Id.

242. See Kesan & Hayes, supra note 235, at 418–19 (“It is almost impossible to accurately and consistently identify attackers, which severely complicates any steps that might be taken to uncover those responsible and hold them accountable for their actions.”).
deterrence through fines or jail time are diluted for a number of reasons. 243 Perpetrators can attack from almost anywhere on the globe, creating jurisdictional impediments and discouraging even the beginnings of an investigation. 244 Furthermore, evidence linking a crime to a particular person is often lacking. 245 Businesses victimized by security breaches are also reluctant to report breaches in the first place. 246 Many of these cyber threats against businesses target personal information. 247 Even if personal information is not the object of the attack, it is often used or otherwise compromised, as evidenced by the Saudi-Israeli cyber-feud described above. 248

Consumers that entrust companies with their personal data find themselves at risk due to data security failure. In 2011, hackers stole the names, addresses, and passwords of over 100 million consumers when they broke into Sony’s servers. 249 Epsilon, an email marketing provider, acknowledged similar breaches. 250 Such attacks demonstrate the inverse relationship between data privacy and data security. Without one the other does not exist; without security in the commercial market, consumers’ bank accounts, spending patterns, health records, political, and religious associations are exposed.

243. See id. (stating that “law enforcement and judicial action against malicious cyber intrusions currently do not present enough of a practical threat to deter potential attackers”).

244. See Calkins, supra note 239, at 183–84.


246. See Krause, supra note 245, at 52 (noting a survey in which only 34% of companies that had their computer security breached reported it to law enforcement); Lawrence A. Gordon et al., 2004 CSI/FBI Computer Crime and Security Survey 13 fig.20 (2004) (estimating that only 20% reported after data breaches).

247. See, e.g., Schwartz, supra note 232.


B. U.S. Response to the Threat Landscape

Despite pervasive and accelerating cyber threats, the FBI finds that organizations continue to ignore them, nothing that: "Either they don't recognize it, they don't understand it or they don't care." Perhaps some organizations fit that description, but recent surveys reflect that Americans are very concerned about their personal data, both on and off the Internet. What has been done to address pervasive security threats?

In May 2010, the Pentagon instituted U.S. Cyber Command, headed by General Keith B. Alexander, director of the National Security Agency. The United Kingdom has a similar operations center, but both cyber commands protect only military installations and assets, leaving other government and corporate interests under the protection of the Department of Homeland Security and private security entities.

Much like privacy regulation, no comprehensive legal standard governs how individuals and non-public organizations must secure consumer data. A series of statutes, regulations and industry self-regulation create the cobbled defenses of U.S. corporate infrastructure. The Safeguard Rule serves as a prime example. Promulgated by the FTC pursuant to the Gramm-Leach-Bliley Act, the Safeguard Rule requires a specific data security plan but applies only to certain financial institutions. Similarly, the

---

251. Smith, supra note 214.
256. See Thompson, supra note 7, at 477–80; Arvind Narayanan & Vitaly Shmatikov, Privacy and Security Myths and Fallacies of “Personally Identifiable Information”, 52 VIEWPOINTS 1, 6 (2010) (noting that “there is no overarching federal law regulating private entities”).
257. See Thompson, supra note 7, at 477 (“Yet a review of the current legal and regulatory landscape reveals that these modern technological threats are being crudely addressed with old-world tools that are incapable of producing the desired results.”).
258. See SOTTO, supra note 50, § 3.02.
Health Insurance Portability and Accountability Act requires reasonable security, but only for certain medical data.\(^{259}\)

The payment card industry provides a good example of industry self-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.\(^{260}\) States also create data security obligations. Breach notification statutes are increasingly popular among the states.\(^{261}\) 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.\(^{262}\)

While U.S. data security regulations are similar to U.S. privacy regulations in their sectoral application, they are markedly less stringent. Moreover, security regulations, like breach notification laws, simply require certain organizations to maintain data security; they do not say how to do so, or provide specific allowances for data processing for security purposes. The legal landscape is fairly characterized as industry-specific, disparate, and inadequate, especially given increased governmental recognition and widespread concern over cybercrime.\(^{263}\)

### C. Exceptions for National Security

Interestingly, national governments enjoy broad exemptions from data privacy regulation when processing data for security purposes. Article Three of the Directive states that: "This Directive shall not apply to . . . processing operations concerning public security, defense, State security . . . and the activities of the State in areas of criminal law."\(^{264}\)

The U.S. federal government has taken full advantage of this exemption. Even before the Pentagon created U.S. Cyber Com-


\(^{261}\) Abraham Shaw, Data Breach: From Notification to Prevention Using PCI DSS, 43 COLUM. J.L. & SOC. PROBS. 517, 519 (2010); SOTTO, supra note 50, § 15.02.


\(^{263}\) See Thompson, supra note 7, at 477–80; Narayanan & Shmatikov, supra note 256, at 6.

\(^{264}\) See Data Protection Directive, supra note 14, art. 3(2).
mand in 2010,\textsuperscript{265} it revealed expenditures of over $100 million in responding to cyber-attacks.\textsuperscript{266} But Cyber Command and these Pentagon expenditures protect military assets rather than other government or private infrastructures.\textsuperscript{267}

How should private interests be protected? The question implicates at least two others: (1) Does the Directive’s exemption that allows national governments to process personal data for public security extend to a nation’s efforts to protect private enterprise?; (2) If so, is it desirable to concentrate all Internet security powers and obligations into one entity, the national government?

Despite segregated security for the military, the United States at least envisions a private partnership to secure non-military data. The Comprehensive National Cybersecurity Initiative, established in 2008,\textsuperscript{268} directed the Executive Branch “to work closely with all key players in U.S. cybersecurity, including state and local governments and the private sector.”\textsuperscript{269} The goal of “articulating roles for private sector and international partners”\textsuperscript{270} is overshadowed, however, by the Initiative’s deployment of a wide-ranging intrusion detection and monitoring system. Federal detection systems, Einstein 2 and Einstein 3, perform several functions, including monitoring Internet traffic for “unauthorized access and malicious content.”\textsuperscript{271} At present, these systems do not defend commercial or civilian networks,\textsuperscript{272} although some advocate the need to do so in the near future.\textsuperscript{273} In fact, the government’s commitment to keep such monitoring devices out of the commercial Internet is belied by a recent interview with a Homeland Security official, who

\begin{footnotes}
\begin{enumerate}
\item \textsuperscript{265} Brito & Watkins, supra note 253, at 70–71; U.S. Gov’t Accountability Office, Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative 1 (2010); Cyberwar, ECONOMIST (July 1, 2010), http://www.economist.com/node/16481504?story_id=16481504&source=features_box1.
\item \textsuperscript{266} Brito & Watkins, supra note 253, at 70–71; Micah Schwalb, Exploit Derivatives & National Security, 9 YALE J.L. & TECH. 162, 166 (2007).
\item \textsuperscript{267} See Cyberwar, supra note 265.
\item \textsuperscript{270} Id.
\item \textsuperscript{271} Id.
\item \textsuperscript{272} See Satola & Judy, supra note 31, at 1759 (noting that Einstein 3 is currently being deployed on a limited pilot program basis and adds the additional capability to do real-time, full, deep-packet inspection and to respond appropriately to cyber-threats before harm is done, providing an intrusion prevention system supporting dynamic defense).
\item \textsuperscript{273} See, e.g., Young, supra note 255, at 174, 176.
\end{enumerate}
\end{footnotes}
said the agency was considering installation of Einstein 3 to non-

While cyber threats are real and growing, they do not justify pervasive government censorship.\footnote{275. See David W. Opderbeck, \textit{Cybersecurity and Executive Power}, 89 \textit{Wash. U. L. Rev.} 795 (2012) (arguing that while threats posed by cybercrime, cyberwarfare, and cyberterrorism are significant, the threats to civil liberties posed by current legislative cybersecurity proposals are equally real and that many congressional efforts to increase cybersecurity are misguided).} The U.S. “Kill Switch” Bill, as it is colloquially known, illustrates the type of overreaction to cyber security problems implicit in granting a single entity sole responsibility for data security.\footnote{276. See Thompson, \textit{supra} note 7, at 491; Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. §§ 102(a), 246, 249(a) (2010); see also Declan McCullagh, \textit{Internet ‘Kill Switch’ Bill Will Return}, \textit{CNET News} (Jan. 24, 2011), http://news.cnet.com/8301-31921_3-20029282-281.html?tag=topStories1.} The controversial bill would grant the President emergency powers over much of the Internet without judicial or congressional preapproval.\footnote{277. See S. 3480 §§ 102(a), 246, 249(a); David W. Opderbeck, \textit{Cybersecurity and Executive Power}, 89 Wash. U. L. Rev. 795, 804 (2012) (presenting an analysis of the constitutional authority of the President to shut down or limit public access to the Internet in a time of national emergency).} The bill would empower the President to force private operators of critical infrastructure to implement emergency plans, including stopping data flow.\footnote{278. S. 3480 § 249(a).} Widely criticized, the bill garnered increased scrutiny after the Egyptian government ordered that country’s major Internet service providers to cease routing data during anti-government protests in early 2011.\footnote{279. See Bambauer, \textit{supra} note 11, at 616–21 (citing David Zax, \textit{Could Egypt Happen Here? Obama’s Internet “Kill Switch”, Fast Company} (Jan. 28, 2011), http://www.fastcompany.com/1721753/egypt-internet-kill-switch).}

As one commentator noted, “the underlying concept of the legislation—to allow America to ‘pull up the drawbridge’ in case of a cyberattack—plainly involves substantial augmentation of the government’s control over private Internet infrastructure.”\footnote{280. Id. at 610.} These thick fingered initiatives, exacerbated by alarmist comments,\footnote{281. Michael McConnell, former director of national intelligence, called for a re-engineering of the Internet and a return to a Cold War mentality of deterrence, based on the threat that the United States would massively retaliate against any perceived attack. Mike McConnell, \textit{Mike McConnell on How to Win the Cyber-war We’re Losing}, \textit{Wash. Post} (Feb. 28, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502498.html (“More specifically, we need to re-engineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment—who did it, from where, why and what was the result—more manageable.”).} are
largely reactionary and prompt government to take too singular a role in providing cyber security.\textsuperscript{282}

Ultimately, most data privacy regulations exempt national governments when they process private data for security purposes.\textsuperscript{283} No such exemption allows non-government organizations reprieve from data privacy regulation.\textsuperscript{284} As a result, the responsibility and the power to secure critical data concentrates disproportionately in national government. Legislation that allows one person to "turn off" the Internet, or that condones pervasive monitoring under the guise of security, vitiates as many rights as it protects.\textsuperscript{285} A ground-up and balanced approach to data security that partners private and public measures avoids such laws and affords all parties subject to cyber threats the ability to secure their own computer systems in proportion to individual risk.\textsuperscript{286}

IV. PRIVACY RULES THAT UNDERMINE PRIVACY RIGHTS

The evidence suggests that the threat landscape with regard to Internet security is substantial.\textsuperscript{287} A variety of malware, including viruses, botnets, logic bombs, worms, and Trojan horses—combined with a variety of motivations—create risks of ongoing damage estimated in the tens of billions of dollars in the United States alone.\textsuperscript{289} Worldwide, approximately 25\% of computers connected to the Internet have been compromised.\textsuperscript{290} Internet hacking has increased in frequency and scope.\textsuperscript{291} Attacks are increasingly

\begin{itemize}
  \item \textsuperscript{282} Young, supra note 255, at 186 ("The entire national security sector, including military, government, and commercial network providers, must learn to collaborate in the same way that our cyber adversaries do. There is currently no guidance for the national security sector to resolve conflicts or encourage collaboration between the government and the private sector when faced with network defense or attack.").
  \item \textsuperscript{283} See, e.g., Data Protection Directive, supra note 14.
  \item \textsuperscript{284} See id.
  \item \textsuperscript{285} See Bambauer, supra note 11, at 616–21, 669.
  \item \textsuperscript{286} See Young, supra note 255, at 186.
  \item \textsuperscript{287} See Thompson, supra note 7, at 495 (noting the abundance of evidence that cyber security problems are "both vast and significant"). See generally Symantec, supra note 8.
  \item \textsuperscript{288} See Satola & Judy, supra note 31, at 1748–49 ("Motives for the attacks range from financial gain to the advancement of national security interests, to the satisfaction of peer recognition, and to the advancement of various causes.").
  \item \textsuperscript{289} See U.S. Gov't Accountability Office, GAO-07-705, CYBERCRIME: PUBLIC AND PRIVATE ENTITIES FACE CHALLENGES IN ADDRESSING CYBER THREATS 8 (2007) (using Federal Bureau of Investigation reports to estimate total losses of $67.2 billion in 2005).
  \item \textsuperscript{290} See Nate Anderson, Vint Cerf: One Quarter of All Computers Part of a Botnet, Ars Technica (Jan. 25, 2007), http://arstechnica.com/news.ars/post/20070125-8707.html.
  \item \textsuperscript{291} See Fernando M. Pinguelo & Bradford W. Muller, Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals, 16 Va. J.L. & Tech. 116, 133 (2011) (noting that Microsoft repaired twice as many botnet-infected com-
sophisticated, often coordinated by organized criminal syndicates or by states.

As a result, one might expect regulations protecting privacy and personal information would simultaneously encourage data security and incentivize entities to provide data security. At first blush, it appears privacy regulations do so. The E.U. Directive imposes data security obligations on data controllers. Article 17 states that "the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction." Data controllers must "ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected," a requirement that increases security obligations with the level of data sensitivity.

While such security requirements—embedded within data privacy regulations—appear to address security concerns, they fail to provide the means by which entities can comply. How do data processors and data controllers comply with security mandates? How do they "ensure" an "appropriate" level of security? What if an entity must use personal information in order to secure personal information? As one commentator notes, "it is often difficult to find a clear legal basis for the processing of personal data for network and IT security purposes . . . ."

A. 'Too Much Privacy is No Privacy at All'

The need to balance privacy regulations by allowing for data security has been recognized by a few commentators, even those

puters in 2010 than in 2009); SYMANTEC, supra note 8, at 12 (stating that Symantec blocked more than 5.5 billion malicious attacks in 2011, an increase of more than 81% from 2010).

292. See Pinguelo & Muller, supra note 291, at 134.


295. Id.

296. Id.; see also 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, 349 (2012).


who historically champion data privacy. For example, Kenneth Clarke, the former lord chancellor and secretary of state for justice in the United Kingdom, recently delivered a speech on data protection that took many by surprise. Although recognized as a strong proponent for protecting privacy and a vocal defender of civil liberties, Clarke argued that data privacy cannot exist without better data security, explaining as follows:

[W]e must also guard against regulations or reactions which just invert this old order, that become obsessed with privacy or data protection without recognizing the harm that also results to citizens from failure to share information, as well as from careless stewardship of data. Detailed prescription will not in itself make our citizens safer, or more free, in this complex, modern world.

It is precisely this call to “share information” that comprehensive privacy regulations undermine. In early 2012, Microsoft unveiled a plan to share its wealth of security information openly through a real-time intelligence feed. The initial stage of the program would stream Microsoft’s security information that detects dangerous threats to business partners, private corporations, and domestic and foreign governments. If successful, the second stage calls for sharing the threat intelligence feed with the public. The shared intelligence could significantly bolster international malware protection efforts.

But data privacy stands in the way. The intelligence feed distributes IP addresses of systems infected by large botnets. Under the E.U. Directive, IP addresses are considered personally identifiable information. Significant controversy clouds whether IP

300. Id.
302. See id.
303. Id. (noting that some experts see the intelligence feed as not preventing threats before they arise, but possibly reducing the impact of attacks before they become global problems).
304. Id.
305. Frederick Lah, Note, Are IP Addresses “Personally Identifiable Information?”, 41 S. J. L. & Pol’y Info. Soc’y 681, 696 (2008) (“In WP 148, Opinion 1/2008 on Data Protection Issues Related to Search Engines, the Working Party concluded that both IP addresses and cookies containing a unique ID qualify as personal data. The Working Party stated that unless an ISP is absolutely certain that the data corresponding to a user cannot be identified, all IP addresses should be treated as personal data to be on the ‘safe side.’”).
addresses should be considered personally identifiable information, but the current E.U. law envisions them as such. As a result, privacy law would likely preclude Microsoft's effort to share information as a proactive contribution to worldwide anti-malware initiatives. One expert responded to this phenomena by noting that "we are still too secretive about security issues. The bad guys quickly and widely disseminate information, and defenders must do the same."

1. Protecting Private Data: Evolving Threats

Privacy laws pose an even greater barrier to data security in light of evolving security techniques, many of which require large amounts of data. As malware evolves in complexity and sophistication, so do the security techniques developed to neutralize new threats. If there was legal uncertainty whether personal data could be processed for security purposes five years ago, that uncertainty deepens with the implementation of modern security methods that require increasingly large amounts of data.

Protecting against Internet threats requires at least a generalized understanding of those threats. An attack typically includes reconnaissance, penetration, and concealment, but these phases can be executed through a variety of vehicles. A computer virus, for example, is a program that can replicate itself and spread from one computer to another. It infects a host program, triggers, and spreads by cloning itself, or part of itself, and attaching the new versions to other host programs. Many viruses have a "payload" outfitted to deliver harmful effects, such as deleting, stealing, or modifying digital information. Two decades ago, traditional antivirus technologies shielded users from such attacks. The ubiq-


307. Neagle, supra note 301 ("Microsoft will have to answer to privacy skeptics, especially considering the threat [that the] intelligence feed will distribute IP addresses of systems that are found to be part of large botnets.").

308. Id.

309. See Kuner, supra note 298.


312. See id.

uity of antivirus software catapulted companies like Norton and McAfee to prominence as personal computer sales soared.\textsuperscript{314} Today, the evolving threat landscape precludes reliance on traditional antivirus technologies.\textsuperscript{315} In 2011 for example, Symantec reported 403 million variants of malware.\textsuperscript{316}

One type of attack gaining prominence recently is a "distributed denial of service attack" (DDoS). Rather than gaining unauthorized access or control of a system, denial of service attacks render systems unusable.\textsuperscript{317} By overloading the capabilities of a system or network, denial of service attacks block all users from accessing the network.\textsuperscript{318} The attacks are formed when valid traffic floods a service until there is not enough bandwidth for the service to stay live.\textsuperscript{319} To stop the flood of data, those targeted by DDoS attacks commonly defend against them by taking down their own service or website, which signals a successful attack.\textsuperscript{320} One security company reported over $26 million in losses associated with DDoS attacks in 2004.\textsuperscript{321} The politically-motivated attack that brought down much of Estonia's web-based infrastructure was partly a denial of service attack.\textsuperscript{322} Anonymous, the now infamous group of loosely-connected "hacktivists," targeted the Church of Scientology by unleashing a DDoS attack, temporarily knocking it offline.\textsuperscript{323}

\begin{footnotes}
\item[315.] At the turn of the century, a relatively small number of threats were distributed widely— to millions of machines. See de Villiers, \textit{Enabling Technologies}, supra note 310, at 7–8. Those machines with antivirus technology recognized the malware signature and protected the system. See id. at 9. Today, sophisticated hackers employ a raft of obfuscation techniques, altering the appearance of the threats. See id. at 9–20. Attackers now create a new threat variant in real-time for each victim, resulting in millions of distinct variants. See Symantec, supra note 8, at 16.
\item[316.] See Symantec, supra note 8, at 45.
\item[319.] Id.
\item[320.] Kesan & Hayes, supra note 235, at 431–33.
\item[322.] Katharine C. Hinkle, Countermeasures in the Cyber Context: One More Thing to Worry About, 37 Yale J. Int’l L. Online 11, 15 (2011) ("Widely regarded as retaliation for Estonia’s removal of a statue depicting a World War II Russian soldier, these attacks hobbled many of Estonia’s key commercial and government networks in a staggeringly simple fashion: by making repeated, overwhelming requests for information, known as distributed denial-of-service (DDoS) attacks.").
\item[323.] Kesan & Hayes, supra note 235, at 427 n.53.
\end{footnotes}
Another distinct threat, botnets, include a collection of compromised computers, each of which is known as a “bot” connected to the Internet. The “botmaster” or “bot herder” controls these “zombie” computers and can use them to launch coordinated attacks like DDoS attacks.

In fact, otherwise distinct threats—viruses, DDoS attacks, and botnets—often overlap and work in conjunction with one another. The Conficker worm is an example of such overlap. Starting in late-2008, the Conficker worm exploited vulnerabilities in a number of Microsoft operating systems. Once it takes over and infects a computer, it spreads to other unprotected computers linking them together into a massive botnet that can be directed by its authors, regardless of location. Since its first detection, Conficker has infected millions of computers and business networks in countries around the world. Worms like Conficker typically install “backdoors” in the infected computer, enabling the computer to be remotely controlled.

Of course there are other vehicles that enable hackers to obtain personal data, including Trojan horses, logic bombs, and zero-day attacks. These threats can be launched in an increasing variety of ways, including websites, emails, internal bad actors, smart phones, and zip drives. The variety and diversity of tools available to hackers coupled with user vulnerability via increasing points of entry present an evolving and sophisticated security challenge.

324. See de Guzman, supra note 318, at 528–30.
325. See id.
326. See id. (noting that DDoS attacks often rely on bot nets to execute denial of service); Edwards, supra note 311, at 26 (noting that the characteristics of viruses, worms and Trojan Horses “are becoming intertwined and may now be found in one piece of software”).
328. See id.
329. See id.
331. See Thompson, supra note 245, at 545 n.41 (2009) (describing Trojan horses generally as “harmful functions embedded with more innocuous software”).
332. Id. (describing “logic bombs” generally as harmful pieces of software that execute under specific conditions).
333. Jeremy Richmond, Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?, 35 Fordham Int’l L.J. 842, 853–54 (2012) (“A zero-day hack exposes a vulnerability in a piece of software that was previously unknown to the developer. Since most computers worldwide run Windows, a zero-day Windows hack is quite valuable.”).
334. See de Villiers, Enabling Technologies, supra note 310, at 21.
2. Protecting Private Data: Evolving Methods

Technology users can no longer depend exclusively on firewalls, or simply react to breaches after their system has been infected. Security companies now offer a spectrum of programs and services designed to overlap and collaborate—much like evolving malware. Where traditional file-based protections react to viruses by scanning for known signatures embedded in the malware, modern security offerings seek to monitor entire networks and prevent malicious activity before it enters a user’s system.

Network-based, behavior-based, and reputation-based systems are designed to block attacks before they reach any given system. Network-based protections analyze incoming data streams via network collections. Sometimes called intrusion prevention solutions, network protections work inside the browser, “looking at the network and browser traffic as it is being rendered.” Some technologies track malicious IP addresses and domains, preventing malware and malicious traffic from known malicious websites.

Behavior-based protections defend against web attacks based on program behavior. This approach to malware detection monitors behaviors of a program to determine whether it is malicious or not. Behavior-based protocols usually monitor the

335. See Symantec, supra note 8 (emphasizing “defense in depth strategy” where “multiple, overlapping, and mutually supportive defense systems [ ] guard against single-pint failures in any specific technology or protection method”).

336. See Kelly A. Gable, Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent, 43 Vand. J. Transnat’l L. 57, 95 (2010) (noting that signature-based measures have not been enough and failed “to prevent massive cyberattacks totaling billions of dollars in losses and inestimable damage to national security, as shown in Estonia and more recently in attacks on U.S. government websites”).


338. See Technology: Defense in Depth, Symantec, http://www.symantec.com/about/profile/star_technology.jsp (last visited Nov. 14, 2012) (“Network-based protection is a set of technologies designed to block malicious attacks before they have a chance to introduce malware onto a system. Unlike file-based protection, which must wait until a file is physically created on a user’s computer before scanning it, network-based protection analyzes all incoming data streams before they can processed by the computer’s operating system and cause harm.”).

339. Id.

340. Id.

341. See id.


343. Id.
stream of system calls that a program issues to the computer’s operating system. Generally speaking, a behavior-based technology protects against threats based on what the application does rather than what it looks like. “Because behavior-based techniques monitor what a program does, they are not susceptible to the shortcomings of techniques that only monitor a threat’s identifying signature.”

The move from signature-based detection to behavior and reputation-based protection reflects industry response to evolving threats. Advanced detection methods, however, often require massive amounts of data. Reputation-based models analyze vast networks of traffic, using large amounts of data to compute reputation scores, which are in turn integrated into security products. Information like IP addresses, domain names, and associated domain name system (DNS) records are required to assess the likelihood that a message is spam or otherwise malicious. In other words, contemporary security methods analyze and rely on large amounts of information to monitor and detect threats. Much of that information falls under the E.U. Directive’s definition of personal data.

For example, traffic analysis does not look for harmful code within a particular attack, but culls out other characteristics such as origination, destination, routing, length of the message, time it was

344. Id.
346. See Jha, supra note 342.
347. See STAR Malware Protection Technologies, supra note 345 (“Some years ago, traditional antivirus technologies were all that was needed to protect an endpoint from attack. However, with the dramatic shift in the threat landscape over the last few years, it is no longer reasonable to think that antivirus-based technologies alone are sufficient.”); Jha, supra note 342 (“To combat these types of threats, the industry is moving from signature-based anti-malware to behavior-based approaches.”).
348. See STAR Malware Protection Technologies, supra note 345 (“Using the combined wisdom of over 130 million contributing users, our reputation system learns which applications are good and bad based on the anonymous adoption patterns of our users. It then uses this intelligence to automatically classify virtually every software file on the planet.”).
349. Domain Name System, or DNS, is an Internet technology that converts domain names to IP addresses. The DNS acts as a mediator between IP addresses—the system-side names of the websites and their respective domains—and their user-side alpha-numeric titles. Another important function of the DNS is to control the delivery of email messages.
350. See id. (“Symantec’s reputation-based security takes a totally different approach. It doesn’t just focus on bad files, but attempts to accurately classify all software files, both good and bad, based on countless anonymous telemetry “pings” sent to Symantec every second of every day from around the world.”).
sent, and frequency of the communication. These unique traits are gathered either from network traffic or by firewalls or routers and are processed by data mining techniques to generate alerts and provide useful information to the analyst aiding in the decision on how to allocate analysis resources. Again, much of that information falls under the Directive’s definition of personal data.

A “honeypot” is another security technique that unquestionably “processes” “personal data.” Honeypots are decoys, servers attached to the Internet that lure in potential hackers. Security professionals create such decoys in order to study hacker activity and monitor how intrusions infiltrate various systems. Useful security tools, honeypots reveal a full end-to-end picture of an attack. Analysis can identify pre-attack behavior as well as post-attack actions taken by the intruder, including payloads and root-kits installed after intrusion. But honeypots record all activity occurring on that device. Some have compared it to wire-tapping and entrapment. Regardless, honeypots make no distinction between personal data and non-personal data.

In sum, the threat environment has become so complex and ubiquitous that the most promising security requires overlapping techniques both based on signature recognition and preemptive reputation and network-based protections, colloquially termed “defense-in-depth.” Modern detection and prevention measures require large amounts of data. Data security company Symantec boasts a “Global Intelligence Network” with more than 64.6 million “attack sensors” that record “thousands of events per second” and that “monitor attack activity in more than 200 countries and territories.” Much of the data might be impersonal or anonymous, but given the European Union’s broad definition of personal data that includes automated analysis of IP addresses, modern threat

352. See id.
354. See id. at 319.
355. See id.
356. See id.
358. See SYMANTEC, supra note 8 (recommending “defense-in-depth,” which emphasizes “multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method”).
359. See id.
detection systems in fact “process” “personal data” regularly. As a result, modern techniques that rely on large quantities of data may very well violate international data privacy law.\textsuperscript{360}

\section*{B. An Open Window: The European Union’s Proposed Regulation}

Arguably, some protection systems, like behavior and reputation-based systems, should be encouraged given the threat landscape while others, like honeypots, should be highly regulated.\textsuperscript{361} Instead, all are hobbled by privacy regulation. The current inability of individuals and organizations to protect against cyber threats emasculates data privacy. The Directive includes exceptions to data privacy requirements for national security and criminal investigations, precedents upon which policymakers can rely in carving out an additional exception that would allow private data processing of personal information strictly necessary for data security.

The opportunity for reform is already at hand because the Directive will soon be replaced with updated legislation. After several official reports assessing the Directive’s effectiveness,\textsuperscript{362} the Commission concluded that while the Directive’s core mission remained valid, globalization and technological advancement required substantial revision.\textsuperscript{363} Instead of piecemeal amendments, the Commission proposed a General Data Protection Regulation (Proposed Regulation), that would repeal and replace the Directive.\textsuperscript{364} The Proposed Regulation would likely not be effective until 2015, and much of the regulation’s content will undoubtedly change as the multitude of stakeholders provide additional testimony and recommendations to the draft language.

Where the Directive suffered from disunity, prescribing end results from which twenty-seven Member States draft individualized legislation, the Proposed Regulation bypasses national legislation

\textsuperscript{360} Kuner, supra note 298 (“[I]t is often difficult to find a clear legal basis for the processing of personal data for network and IT security purposes.”).

\textsuperscript{361} See Bambauer, supra note 11, at 587–88 (noting that “cybersecurity policy necessitates difficult tradeoffs, particularly between ensuring authorized access and alteration and preventing unauthorized interaction with data”).


\textsuperscript{363} Françoise Gilbert, Proposed EU Data Protection Regulation: The Good, the Bad, and the Unknown, 15 J. INTERNET L. 20 (2012).

and itself directly binds Member States upon enactment.\textsuperscript{365} There is no need for twenty-seven new legislative texts. The projected unity provided by the Proposed Regulation, however, must be balanced against the substantive changes it envisions.

1. The Proposed Regulation’s Heightened Restrictions on Data Processing

Generally speaking, the European Union’s proposed reform is more restrictive than its predecessor. One commentator notes “the responsibilities of data processors as set forth in Article 26 [of the Proposed Regulation] are much more extensive than those contained in Article 17 of Directive 95/46.”\textsuperscript{366} The Proposed Regulation would erect more obligations for companies, increase accountability for data processors, and levy sharper fines with broader liability for those who fail to comply.\textsuperscript{367} The Proposed Regulation also constricts the definition of consent, allowing only explicit consent before a user’s personal data can be processed.\textsuperscript{368} It further requires organizations to more stringently limit the amount of data they collect.\textsuperscript{369} Data controllers must comply with stricter informational and transparency obligations.\textsuperscript{370} In some cases, organizations must appoint a data protection officer, conduct or pay for data protection impact assessments, and make and retain records of data processing activities.\textsuperscript{371} Overall, the Proposed Regulation “represent[s] a comprehensive revision and strengthening of data protection laws in the E.U., which are already considered to be the most stringent in the world.”\textsuperscript{372}

Not only are the requirements more stringent, they exact a higher price for noncompliance. One commentator notes that “[t]he sanctions that may be imposed on companies under the Proposed Regulation are hugely increased over what was previously possible,” ranging as high as 2% of a company’s annual worldwide revenues.\textsuperscript{373} If a European DPA ruled that Google violated certain provisions of the Proposed Regulation, for example, it could fine

\textsuperscript{365} See Paul Craig & Gráinne de Búrca, EU Law: Text, Cases, and Materials 105-06 (5th ed. 2011).
\textsuperscript{366} Kuner, supra note 298.
\textsuperscript{367} See generally Gilbert, supra note 363.
\textsuperscript{368} Id. at 23.
\textsuperscript{369} See Proposed Regulation, supra note 364, art. 5(c).
\textsuperscript{370} See Gilbert, supra note 363, at 25-30.
\textsuperscript{371} Id. at 27.
\textsuperscript{372} Deloitte, The Modernization of European Data Protection Rules 2 (2012); see also Kuner, supra note 298.
\textsuperscript{373} Id.
Google approximately $580 million—2% of its 2010 revenues.\footnote{Id.} In addition to increased fines, individual data subjects will also be able to bring suit against a controller or processor. The Proposed Regulation includes joint and several liability for data controllers and processors, with each liable for the full amount of any damage suffered.\footnote{Id.}

Like the consequences for noncompliance, the obligations for those who process data increase sharply under the Proposed Regulation, which increases the obligation to keep personal data secure.\footnote{See Proposed Regulation, supra note 364, art. 77(2)-(3).} One proposed provision, for example, adds a disclosure requirement not currently required by the Directive: if a data breach occurs, data processors and controllers must notify both the DPA and the affected data subject within twenty-four hours.\footnote{See Proposed Regulation, supra note 364, arts. 31-32.} Although the new requirements are onerous, one critical provision arguably addresses the need to allow data processing of personal information for security’s sake.

2. The Proposed Regulation’s New Security Provision

The provision recognizing the need to process information for security reasons is not an exemption, although an argument could be made that processing personal data for the exclusive purpose of maintaining informational security should be an exemption. Exemptions, instead, are limited to the investigation and prosecution of crimes\footnote{See id. art. 2.} and national security.\footnote{But see Kuner, supra note 298.} Rather than afford a similar exemption for data processed solely for informational security reasons, the Proposed Regulation provides in Article 6 and Recital 39 that data processing for network and information security is to be considered a “legitimate interest.”\footnote{Id. But see Kuner, supra note 298 (“It is not clear which, if any, data protection rules would govern ‘national security,’ which is presumably left to national law.”). There are also limited exemptions for journalistic purposes, artistic and literary expression. See Proposed Regulation, supra note 364, art. 80.}

In particular, the new law provides as follows:

Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: . . .

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests
are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.381

Standing alone, this language provides little comfort to those seeking legal authority to process personal data for informational security purposes. Recital 39, however, gives context to Article 6(f):

The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping “denial of service” attacks and damage to computer and electronic communication systems.382

Data controllers, in other words, have a legitimate interest in processing information for security purposes, which means that a balance of interests test will determine the legality of such data processing. While unclear in application, this provision at least recognizes the evolving threat environment and the concomitant need for security allowances.383 Balancing tests are inherently uncertain in application,384 a fact recognized by the Commission, which has already signaled its intent to clarify the use of the balancing of interests test.385 Nonetheless, one commentator suggests that “it is unclear how the Commission can produce guidance that is both authoritative and specific enough to be useful”; a potentially prescient observation.386

381. Id. art. 6(1)(f).
382. Id. pml. ¶ 39.
383. Kuner, supra note 298 (noting that under the Directive, “it is often difficult to find a clear legal basis for the processing of personal data for network and IT security purposes”).
385. See Kuner, supra note 298.
386. Id.
When Fortune 500 companies and entire governments cannot keep data private or protected from variant cyber threats, a clear exemption legitimizing data processing for security is needed. Nebulous balancing inquiries cloud the circumstances in which data may be processed for informational security purposes. Even so, Recital 39, if in fact enacted, is a step in the right direction. Recital 39 represents an understanding that personal data remains vulnerable without adequate security, and that privacy laws that restrict processing and sharing of personal data for security purposes undermine data privacy by increasing its vulnerability.

That is not to say organizations should have free reign to process any and all data under the guise of providing security.\textsuperscript{387} Companies that specialize in providing data security should be required to limit their use of personal data to information technology and network security only, which would help assuage privacy concerns about misuse and overreaching. Similarly, periodic audits of data security processing could ensure that personal data is not being used for illicit purposes.

Importantly, the measures outlined above from the Proposed Regulation are not set in stone. Opportunities for alterations and modifications remain. To balance the lopsided emphasis on data privacy, language like that in Article 6 and Recital 39 should be retained and strengthened.

V. Conclusion

Data privacy and data security share a symbiotic relationship. Allowing unregulated monitoring of the Internet in the name of security emasculates privacy; and privacy laws that restrict all data processing—including processing for security purposes—undermine privacy, by leaving personal data unprotected. When hackers can infiltrate Citigroup and expose customers' financial data, cyber criminals can steal millions of Sony customer files, and Saudi Arabian nationals can illegally access and reveal credit card information of Israeli nationals, data privacy suffers for lack of data security.

Despite the symbiotic relationship between security and privacy, the international regulatory climate is imbalanced. Privacy regulation worldwide continues to spread without concomitant allowance

\textsuperscript{387} See Bambauer, supra note 11, at 587-88 (noting that "cybersecurity policy necessitates difficult tradeoffs, particularly between ensuring authorized access and alteration and preventing unauthorized interaction with data").
for data security. Individuals and private organizations, as compared with national governments, labor under increasingly burdensome privacy laws while simultaneously defending against sophisticated cyber-attacks. Although data privacy regulations require "reasonable security," the regulations include no exception for the provision thereof. As a result, data security techniques that process personal data may very well violate privacy law, an outcome exacerbated by the advent of modern security methods, which require massive amounts of data.

The call to balance international data privacy law is not, at its core, a radical one. It is not a veiled attempt to consolidate more regulatory power in national government. Instead, it highlights individuals and organizations that are beholden to limitations not visited upon national government. The fact that one of the world's most stringent data privacy laws will soon be revised to include a measure that allows the processing of personal data for security purposes, reflects the real impact that ineffective security has on data privacy.