Drawing the Line Between Competing Interests: Strengthening Online Data Privacy Protection in an Increasingly Networked World

LORI CHIU*

TABLE OF CONTENTS

* J.D. Candidate 2014, University of San Diego School of Law; B.A. 2009, University of California, Irvine. I am extremely grateful to Professors Lisa Ramsey and Junichi Semitsu at the University of San Diego School of Law and Professor Lee A. Bygrave at the Norwegian Research Center for Computers and Law for their valuable insight and guidance in preparing this Article.

I. INTRODUCTION

Online data security is one of many areas of the law in which Congress, the President, and the courts must work together to balance various interests at stake. The Government shoulders the burden of balancing the delicate interests of protecting personally identifiable information[1] while providing businesses with a cost-effective way to protect such data.[2] The first interest to consider is the interest of the individual. The right to privacy must be respected with regard to the sensitive personal information of consumers. Such personally identifying information can include credit card numbers, billing addresses, and login and password information used by consumers when completing online purchases or perusing social networking websites. Personally identifying information can also include employees' personal data that an entity or corporation may store for administrative purposes, but may be susceptible to hackers or other unauthorized user access. With regard to protecting such sensitive online data, the Government must also consider the interests of both large and small businesses to determine the most cost-effective yet least intrusive policies regarding data collection for businesses to put in place.

Unlike the European Union ("EU") model, where data privacy is considered a protected right, United States ("U.S.") data privacy rights

1. "The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Memorandum from John Clay III, Deputy Dir. for Mgmt., Office of Mgmt. & Budget, to the Heads of Exec. Dep'ts & Agencies 1 (May 22, 2007) *available at* http://www.whitehouse.gov/sites/default/omb/memoranda/fy2007/m07-16.pdf.

2. *See* Andrea M. Matwyshyn, Data Devolution: Corporate Information Security, Consumers, and the Future of Regulation, 84 CHI-KENT L. REV. 713, 714–15 (2010).

are founded on principles of tort and contract law.[3] Currently, U.S. data privacy protection stems from a hodgepodge of laws originally drafted for the government and specific sectors of the economy.[4] Congress did not pass many of these laws to apply to information gathered online, but over time, they have been used to regulate data privacy.[5] In the private sector, however, technical and corporate data infrastructures that permit routine collection, maintenance, use, and disclosure of personal information are already in place and expanding. Such infrastructures thereby call for additional privacy considerations beyond currently existing laws.[6]

In the past decade, the nature of personal data flows has experienced a dramatic shift to a new paradigm—data access—whereby individuals can access information via global web technologies.[7] As a result, an individual's personal data has become a commodity and has changed the way companies do business.[8] Due to the rapid advancement of technology, businesses are now able to collect personally identifying information from Internet users and use it in complex ways such as targeted commercial marketing.[9] Although such technological advancement benefits businesses by allowing such sensitive personal information to flow freely across the web, such changes also bring serious risks to consumers, primarily due to breaches of personal privacy as a result of the increased availability of personally identifying information to private companies.[10] Information crime through identity theft is one of the most rapidly growing white-collar crimes in the U.S., and consumers frequently make complaints to the Federal Trade Commission regarding identity theft.[11] Furthermore, it has become a well-developed domestic activity for businesses to exploit the use of personal information for business purposes such as commercial

3. Carolyn Hoang, In the Middle: Creating a Middle Road Between U.S. and EU Data Protection Policies, 32 J. NAT'L ASS'N ADMIN. L. JUD. 810, 818 (2012).
4. *Id*.
5. *Id.*
6. *See* Symposium, *Can Privacy be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 149 (1996).
7. Damon Greer, *Privacy in the Post-Modern Era: An Unrealized Ideal?*, 12 SEDONA CONF. J. 189, 190 (2011).
8. *See* Amanda C. Border, *Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States*, 35 SUFFOLK TRANSNAT'L L. REV 363, 363 (2012).
9. *Id.*
10. *Id.*
11. *See* Matwyshyn, *supra* note 2, at 713.

marketing.[12] Accordingly, it is necessary for the federal government to address what rules will apply to the private sector and how the federal government will enforce these rules.

This Article seeks to elucidate these issues and provide a roadmap for the U.S. government to create unified federal laws to provide the private sector with specific protocols regarding use and dissemination of consumer personal information. First, this Article will provide an explanation of the U.S.'s current sector-by-sector approach to regulating personally identifying information and will provide a case study of the Federal Trade Commission's ("FTC") enforcement action against a social networking site in 2011 as one example of the FTC's recent efforts at regulating online privacy. Next, this Article will analyze the U.S.'s current challenge of judicial enforcement of privacy laws in federal courts and will address recent efforts by Congress, the White House, and the FTC to develop comprehensive online privacy legislation. Third, this Article will discuss the European Union's approach to data protection, including such legislation as the 2012 E.U. Proposed Data Protection Directive.

Fourth, this Article will provide specific recommendations for strengthening U.S. data protection policies to address new technologies that have surfaced since the inception of U.S. federal and state online privacy laws. These recommendations include passing uniform federal legislation that will include provisions that model the EU's recent approach to data protection. Such legislation should establish a data controller within both the public and private sectors and require both public and private entities to provide transparent disclosures to consumers regarding the type of information the entity plans to collect and what purposes the entity will use the information for. Additionally, such legislation should require companies to obtain affirmative consent from consumers prior to collecting personally identifying information. Legislation should also provide consumers with a "right to be forgotten" that would mandate entities to stop tracking the consumer's personal information when requested.

Finally, this Article will propose that the FTC work with industry leaders within business communities to adopt industry specific codes of conduct that businesses can voluntarily opt into by self-certifying their compliance with such codes of conduct. In doing this, the U.S. can more effectively balance individual, community, and governmental interests in the area of data protection and ensure that both individuals and entities are on the same page with regard to the collection and use of the personally identifying information of consumers.

---

12. *See generally id*.

II. CURRENT U.S. DATA PROTECTION REGULATION

The rationale behind the U.S. "sector" specific model of data protection is that it would be better for businesses to regulate themselves than to have the government intervene in their affairs.[13] Although businesses would be regulated by some laws, for the most part, businesses themselves would decide how to implement data protection.[14] Indeed, state and federal regulatory laws are only one component of the U.S. informational privacy policy.[15] At present, federal laws protect citizens and provide a cause of action against companies that unlawfully obtain their personal data in several areas. These areas include credit card and health related transactions, among others. Additionally, aside from such laws, U.S. informational privacy policy also provides the Federal Trade Commission with the power to enforce such laws through prosecution and application of enormous penalties. After illuminating the current state of the law in each of these areas, this Article will discuss the key issue of how U.S. data protection policies have failed to address recent challenges presented by online commercial marketing transactions and consumer use of new online technologies adequately.

A. Federal and State Regulation of Personally Identifying Information

The U.S. approaches the regulation of personally identifying information through a combination of statutes at the federal and state levels. Such regulation focuses on securing the personal information of consumers, such as bank account numbers and addresses, to ensure that the information is adequately protected from hackers that might breach the collecting entity and access this data. Such regulation is also enacted to ensure that the entity does not misuse such information to its own benefit or accidentally release sensitive information due to inadequate security protocols. Such laws set a legal standard that focuses on finding a process to identify and implement measures that are reasonable under the circumstances to achieve the desired security objectives.[16]

13. *See* Hoang, *supra* note 3, at 818.
14. *Id.*
15. *Id.*
16. *Id*. at 819.

With respect to federal and state data protection laws, the type of law depends heavily on the type of information that must be protected. For example, in the finance industry, the Gramm-Leach-Bliley Act declares that it is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the confidentiality and security of those customers' nonpublic, personal information.[17] In the health industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") strictly protects consumer health information by authorizing the Department of Health and Human Services to promulgate regulations relating to the protection of such data.[18] HIPAA requires medical providers, insurers, and other entities handling health information to adopt a system for notice, opt-out-disclosures, and access to private information.[19] The Act also requires secure transmission of health data.[20]

Although these areas of personal data are regulated at the federal level, some areas are regulated at the state level, such as the personal information of consumers making purchases in the retail and sales industries. The Song Beverly Credit Card Act, which prohibits corporations and retailers from storing and using any personally identifying information of the cardholder beyond the last four digits of the credit card, provides one example.[21] Although these laws have been effective in ensuring minimum data security standards for specific entities such as hospitals, banks, and credit reporting agencies, such laws are so specifically tailored that they cannot be applied to newer forms of data storage such as those companies use to collect and monitor consumer information.

In March 2012, the FTC released a report ("the Report") detailing the current state of privacy regulation in the U.S.[22] In its Report, the FTC focused on the fact that self-regulation of data privacy and security has not gone far enough. For example, the FTC's recent survey of mobile applications marketed to children highlighted that many such applications fail to provide any disclosures to users about the extent to which they

---

17. 15 U.S.C. § 6801 (1999).

18. *See generally* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201 (2012).

19. *See* JONATHAN K. SOBEL ET AL., *The Evolution of Data Protection as a Privacy Concern, and the Contract Law Dynamics Underlying It*, in SECURING PRIVACY IN THE INTERNET AGE 55, 58 (Anupam Chander, et al. eds., 2008).

20. *Id.* at 58–59.

21. CAL. CIV. CODE § 1747 (West 2012).

22. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) [hereinafter Recommendations], *available at* http://www.ftc.gov/os/2012/03/129326privacyreport.pdf.

collect and share consumers' personal data.[23] Moreover, as the Report noted, efforts of the data broker industry to establish self-regulatory rules concerning consumer privacy have also fallen short.[24]

The Report also highlighted that there is widespread evidence of data breaches related to consumer information, and noted that published reports have demonstrated that various breaches may have resulted from companies' unintentional release of consumer data.[25] Accordingly, the FTC Report reached two conclusions: first, companies that do not intend to undermine consumer privacy merely lack sufficiently clear standards to operate while respecting consumer expectations; and second, companies that seek to cut corners with respect to consumer privacy do not face adequate legal barriers deterring such behavior.[26]

The FTC's report demonstrates the need for the President and Congress to address these conclusions and provide companies in the private sector with clear standards to operate while respecting consumer expectations. Additionally, the Report also recommends revisiting the current hodgepodge of "sector" specific laws and inconsistent regulation within the data security arena in order to deter companies from cutting corners when handling online data, and to secure the personally identifying information of consumers.

B. Recent Efforts at Online Privacy Regulation by the Federal Trade Commission

Since 2009, the President, Congress, and the FTC have been working in their individual capacities to develop and enact comprehensive online privacy legislation that would protect consumers who use the Internet for social networking purposes, online commercial transactions, or information acquisition.[27] In response to consumer complaints regarding online identity theft and widespread dissemination of personally identifying information of consumers such as e-mail and home addresses, the FTC has launched

23. *Id.* at 11; FED. TRADE COMM'N STAFF, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING 2, 12–13 (2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
24. Recommendations, *supra* note 22, at 11–12.
25. *Id.* at 12.
26. *Id.*
27. Greer, *supra* note 7, at 191.

several enforcement lawsuits against prominent companies under the "deceptive practices" prong of the FTC Act over the last five years.[28]

The regulation of unfair trade practices under Section 5 of the FTC Act serves as one approach to regulation of online data protection.[29] Following a data breach by a corporation, the FTC can impose monetary fines, mandate the creation of security and privacy programs, and monitor such programs for a substantial amount of time to ensure the corporation's compliance.[30] FTC scrutiny can be triggered by a variety of factors, such as a material misrepresentation in a corporation's privacy policy, inadequate safeguards for securing personally identifying information, and unauthorized third party access to consumers' personally identifying information.

In August of 2011, the FTC launched an enforcement action against Facebook.com ("Facebook"), alleging that Facebook had violated the FTC Act through its deceptive privacy policies.[31] The complaint alleged eight separate counts of unfair and deceptive practices by Facebook.[32] Count 1 alleged that Facebook expressly or impliedly represented to users that through their Profile Privacy Settings users could restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends."[33] In many instances, however, the users could not exercise such control over their Profile Privacy Settings, and user information was accessible by Platform Applications.[34]

Counts 2 and 3 each related to Facebook's updated privacy policy, which launched on December 8, 2009 ("the December Privacy Changes"), and changed its existing policy to designate certain user information as "publicly available" ("PAI").[35] Following the December Privacy Changes, users could no longer use their Profile Privacy Settings to limit access to their Friends List, nor use their Search Privacy Settings to restrict access to their Profile Picture and Pages from other users.[36] Facebook implemented the December Privacy Changes by requiring each user to click through a multi-page notice called the Privacy Wizard, which informed users that they were required to choose, via a series of radio

28. Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce." The prohibition applies to all persons engaged in commerce, including banks. *See* 15 U.S.C. § 45 (2012).

29. Michael Kearney, *Legal Trends in Protecting Personal Information*, 7 A.B.A. SCITECH LAW. 20, 20 (2011).

30. *Id*.

31. *See* Complaint, In the Matter of Facebook, Inc., F.T.C. File No. 092 3184 (2011).

32. *Id.*

33. *Id.* at 6.

34. *Id.* at 6–7.

35. *Id.* at 7.

36. *Id.*

buttons, to implement either the new settings that Facebook recommended, or to retain the "Old Settings" for ten different types of profile information.[37]

Count 2 of the FTC's enforcement action alleged that Facebook had engaged in a deceptive act or practice by failing to adequately disclose to users, via the Privacy Wizard notification, that they could no longer restrict access to their name, profile picture, gender, friend list, pages, or networks by using privacy settings previously available to them, and failed to adequately disclose the fact that the December Privacy Changes would override their existing user privacy settings.[38] Count 3 alleged that Facebook materially changed its promise to users and retroactively applied the December Privacy Changes without their informed consent, in a manner that was likely to cause substantial injury to consumers, that was not outweighed by the countervailing benefits to consumers, and was not reasonably avoidable by consumers.[39]

Counts 4 through 7 of the enforcement action related to Facebook's deceptive practices with regard to disclosing user information, such as information included in user personal profiles, as well as user photos and videos, to Platform Applications and advertisers.[40]

In November of 2011, following a full investigation by the FTC, Facebook entered into a settlement agreement that contained a consent order with the FTC.[41] The settlement agreement contained five main provisions.[42] First, the agreement barred Facebook from making any future misrepresentations about the privacy or security of consumers' personal information.[43] Second, it required Facebook to obtain affirmative express consent from consumers prior to enacting any changes that would override users' privacy preferences.[44] Third, Facebook was required to prevent anyone from accessing a user's personal information more than thirty days following the user's deletion of his or her account.[45]

---

37. Such information included profile information such as the user's photos and videos, date of birth, and listings of family and relationships. *Id.* at 7–8.
38. *See id*. at 8.
39. *Id*. at 9.
40. *Id*. at 10–17.
41. *See* Agreement Containing Consent Order, In the Matter of Facebook, Inc., F.T.C. File No. 092 3184 (2011).
42. *Id*.
43. *Id*. at 4.
44. *Id*. at 4–5.
45. *Id*. at 5.

Fourth, the agreement required Facebook to establish and maintain a comprehensive privacy program designed to address privacy risks associated with new and existing products and services.[46] Finally, the agreement required Facebook, within 180 days and every two years after that for the next twenty years, to obtain independent, third party audits certifying that it has a privacy program in place that either meets or exceeds the requirements of the FTC order.[47]

The Facebook case demonstrates the importance of and the need for comprehensive online privacy legislation and regulation. Because Facebook did not adequately disclose the user information that would be stored and shared with third party applications, users were not informed and did not provide affirmative express consent to policy changes. As a result, user personal information such as photos, user IDs, and user employer names was shared with third party applications and advertisers.[48] By bringing the enforcement action, the FTC and advocates in the privacy arena were victorious in their efforts at forcing Facebook to make changes to increase transparency and reduce third party access to user information.[49] Furthermore, by doing so, they paved the way for the FTC to bring future enforcement actions and started a discussion among the consumer and business communities regarding online privacy issues.[50]

Information vulnerability places businesses at risk of both criminal prosecutions and civil law suits for data breaches, and threatens potential losses of key corporate assets.[51] Computer code serves as both a sword and a shield to control information between criminals and technologists, and limited progress has been made in this arena, with even major technology companies, such as Microsoft, stating outright that a regulatory intervention is necessary.[52] Although the FTC continues to regulate the protection of consumer online data through enforcement actions similar to those seen in the Facebook enforcement action, it is essential for Congress to enact federal legislation related to online privacy to provide corporations like Facebook with clear guidelines regarding the collection, storage, and dissemination of consumer personal data.

---

46. *Id*.
47. *Id*. at 6–7.
48. *See* Complaint, *In the Matter of Facebook, Inc.*, F.T.C. File No. 092 3184 at 10–13, 16–17 (2011).
49. *See* Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U.REV. L. & SOC. CHANGE 215, 263–64 (2012).
50. *Id.*
51. *See* Matwyshyn, *supra* note 2, at 714–15.
52. *Id.*

C. Issues with Judicial Enforcement in Federal Courts

Due to the Internet's omnipresent nature, data is often transmitted across several jurisdictions and rarely remains in only one jurisdiction.[53] Because the Internet, social media, and Cloud computing cross national borders, data may be transmitted to nearly any location in the world, leading to privacy problems that are not restricted to any single jurisdiction.[54] As such, several transnational issues may arise within the data protection arena. First, different laws may apply across different jurisdictions and different countries, creating a need for safe-harbor agreements between the U.S. and other countries.[55] Second, enforcement of laws may be difficult because a court may not have personal jurisdiction over the parties due to the movement of data from one jurisdiction to another. Finally, laws may require different elements of proof that the parties must plead in particular suits, which may be difficult for consumer plaintiffs to meet due to the movement of data or due to the plaintiffs' inability to determine how their sensitive personal information such as credit card numbers may be used by hackers.

Because of the continually evolving nature of U.S. online privacy protection, it is difficult for consumers to achieve judicial redress for injuries they sustain when corporations utilize their corporate data infrastructure for commercial marketing purposes. It is also difficult for consumers to succeed in lawsuits when enterprises release sensitive, personally identifying information to third party platforms and applications, whether inadvertently because of inadequate data security protocols or because of hacker infiltration of weakly protected data storage systems. In order to demonstrate standing in data breach cases filed in federal

53. Christopher Wolf & Winston Maxwell, *So Close, Yet So Far Apart: The EU and U.S. Visions of a New Privacy Framework*, 26 ANTITRUST 8, 8 (2012).

54. *Id.*

55. The U.S.-EU Safe Harbor Framework is one example of this. The Safe Harbor Framework was negotiated by the U.S. Department of Commerce in consultation with the European Commission to develop a "safe harbor" framework in order to bridge the differences between the U.S. and EU approaches to data protection regulation. The U.S.-EU Safe Harbor Framework, which was approved by the EU in 2000, provides an avenue for U.S. organizations to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by EU member state authorities under the EU member state privacy laws. By voluntarily self-certifying to the U.S.-EU Safe Harbor Framework, an organization signifies to member EU organizations that it provides "adequate" privacy protection, as defined by the European Commission's Directive on Data Protection. *See* U.S.-European Union Safe Harbor Overview, EXPORT.GOV (Apr. 26, 2012), http://export.gov/safeharbor/eu/eg_main_018476.asp.

court, consumer plaintiffs must demonstrate injury-in-fact.[56] However, if plaintiffs are unable to show evidence that the data breach resulted in actual misuse of the personal information that was accessed, they may face barriers to receiving any recovery, as courts are less likely to find injury-in-fact.[57] Without concrete evidence of identity theft via, for example, evidence of fraudulent use of the plaintiff's credit card or other fraudulent use of personal information that was inadvertently released, federal appellate courts are split on how to approach a plaintiff's allegation that she faces an increased risk of harm following a data breach.[58]

One example of consumer plaintiffs facing major hurdles to recovering for injuries based on the release of their personal information is seen in Krottner v. Starbucks Corp. In that case, the Plaintiff-Appellants were three Starbucks employees whose names, addresses, and social security numbers, along with those of approximately 97,000 other employees, were stored on a laptop that was stolen from Starbucks.[59] After the laptop was stolen, Starbucks informed the employees that the theft had occurred, and stated that they had "no indication that the private information ha[d] been misused," but that as a precaution, Starbucks recommended that employees monitor their financial accounts for suspicious activity.[60] Additionally, Starbucks offered affected employees credit watch services for one year free of charge.[61]

Approximately one month after the theft occurred, Shamasa, one of the Plaintiff-Appellants, was notified by his bank that someone had attempted to open a new account using his social security number, but that the bank had closed the account.[62] The Appellants subsequently filed two putative class action complaints against Starbucks, alleging negligence and breach of an implied contract.[63] Following the filing, the district court granted Starbucks's motion to dismiss, and held that although Plaintiff-Appellants had standing under Article III, they "had failed to allege a cognizable injury under Washington law."[64] On appeal, the Ninth Circuit held that the Appellants had Article III standing, noting

---

56. *See* Kim Pham, *Assessing Risk: Data Breach Litigation in U.S. Courts*, THE PRIVACY ADVISOR, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Nov. 1, 2012), https://www.privacyassociation.org/publications/2012_11_01_assessing_risk_data_breach_litigation_in_u.s._courts.
57. *Id*.
58. *Id.*
59. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140 (9th Cir. 2010).
60. *Id.* at 1141.
61. *See id.*
62. *Id.*
63. *Id.*
64. *Id.*

that if a plaintiff faces "a credible threat of harm," and that harm is both "real and immediate, not conjectural or hypothetical," the plaintiff has met the injury-in-fact requirement for standing under Article III.[65] The court found that the Appellants had alleged "a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."[66]

In contrast to the Ninth Circuit's approach, the Third Circuit has taken a different approach to determining standing in data breach cases, as seen in Reilly v. Ceridian Corporation.[67] In that case, law firm employees brought a putative class action against a payroll-processing firm, alleging claims related to an increased risk of identity theft and seeking costs they incurred as a result of monitoring credit activity after the law firm suffered a security breach.[68] Ceridian was a payroll processing firm that collected information about the law firm's employees including information such as employees' names, social security numbers, dates of birth, and bank account information in order to process its payrolls.[69] At one point, Ceridian suffered a security breach when a hacker infiltrated its online system and potentially gained access to personal and financial information that belonged to Appellants and approximately 27,000 employees at 1,900 companies. It was unknown, however, whether the hacker read, copied, or understood the data.[70] To remedy the breach, Ceridian, like Starbucks, arranged to provide the potentially affected individuals with one year of free credit monitoring and identity theft protection.[71]

Appellants, the law firm employees, subsequently filed a complaint alleging claims including negligence and breach of contract, related to an increased risk of identity theft and alleging that they had incurred costs to monitor their credit activity and suffered emotional distress as a result of the breach.[72] The Third Circuit Court of Appeals affirmed the district court's granting of a motion to dismiss in Ceridian's favor, holding that Appellants' allegations of hypothetical, future injury were insufficient to establish standing, and that Appellant's contentions relied on speculation that the hacker (1) read, copied, and understood their

65. *Id.* at 1143.
66. *Id.*
67. *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40 (3d. Cir. 2011).
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*

personal information; (2) intended to commit future criminal acts by misusing the information; and (3) was able to use such information to Appellants' detriment by making unauthorized transactions in Appellants' names.[73] Regarding Appellants' alleged time and money expenditures to monitor their financial information, the Third Circuit held that they did not have standing because the costs incurred were to monitor a speculative chain of future events based on hypothetical future criminal acts, and were not "actual" injuries.[74]

The breach originally occurred because a hacker accessed Ceridian's online payroll system, but because Ceridian did not have adequate cyber infrastructure to protect from such a breach and did not have technical measures in place to determine whether or not the hacker had actually accessed and copied the employees' information, the Appellants were unable to establish sufficient evidence of "actual injury."[75] Because the Third Circuit did not consider the inadvertent dissemination of Appellants' personal information by a hacker to be an "actual" injury, but rather considered it merely a speculative future injury, Appellants were left with no means of redress for the inadvertent release of their personal information.

Comparing the two cases demonstrates the split that currently exists within the federal courts. Whereas, in *Krottner*, the Ninth Circuit concluded that the risk of future harm following a data breach was sufficient to confer standing, the Third Circuit in *Reilly* characterized the future risk of identity theft as speculative when there was no evidence that the breach was the result of malicious acts and no evidence that there had been any misuse of the compromised personal information.[76] The Third Circuit found the risk to be speculative because Ceridian did not have technological measures in place to determine whether or not the hacker had actually accessed and copied the employees' information for distribution, or if the hacker simply accessed and copied the information and used it for identity theft purposes in another jurisdiction or another country. Such differing outcomes demonstrates the inconsistency in the federal courts and provides an additional hurdle for plaintiffs attempting to recover money they will personally invest in future credit monitoring services in similar cases.

Additionally, although a breach occurred in both cases, the fact that a hacker accessed Ceridian's payroll processing network and obtained employee information was not considered malicious, whereas the theft

---

73. *Id.* at 42.
74. *Id.* at 46.
75. *See id.* at 41–42.
76. *See Krottner*, 628 F.3d at 1143; *see Reilly*, 664 F.3d at 43.

of the laptop in *Krottner* containing employee information was. Moreover, in *Reilly*, the Third Circuit did not take into account the fact that Ceridian's data protection policies may have been weak or inadequate, which could have led to the security breach. The Ninth Circuit may have deemed this malicious on Ceridian's part, just in the same light as it deemed the theft of the laptop containing unencrypted employee data to be malicious in *Krottner*.

The differing outcomes in *Reilly* and *Krottner* further demonstrate the need for the federal government to address online data security regulation within the private sector.[77] Without such uniform federal laws and the imposition of minimum standards such as industry specific codes of conduct regarding the safeguarding of consumer and employee information, it is difficult for courts to determine exactly what personal information was accessed by hackers and whether that information was further disseminated to other hackers, third parties, or the general public. It is also difficult for courts to determine whether plaintiffs in these types of cases face "a credible threat of harm" that is "real and immediate, not conjectural or hypothetical."

By providing minimum standards such as industry codes of conduct for corporations such as Ceridian and Starbucks to apply to their internal cyber infrastructure, the federal government would effectively provide a way for businesses to address these types of data breaches from the outset in order to determine the severity of the data breach and measure the potential that plaintiffs whose data have been compromised will face identity theft in the future. Without such minimum standards, individuals such as the plaintiffs in *Reilly* and *Krottner* may result to "forum shopping" in order to obtain Article III standing or, alternatively, would be forced to rely on the FTC to launch enforcement actions against corporations in order to remedy the effects of dissemination of their personal information.

---

77. In addition to the *Krottner* and *Reilly* cases, other circuit courts have addressed issues of standing in data breach cases and have also come to different results, as seen in *Lambert v. Hartman*, 517 F.3d 433 (6th Cir. 2008) (holding that with regard to governmental dissemination of an individual's private information on a traffic citation, a plaintiff alleging a violation of her right to informational privacy must demonstrate that "the interest at stake relates to 'those personal rights that can be deemed fundamental or implicit in the concept of ordered liberty.'") and *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007) (noting that without more than mere allegations of increased risk of future identity theft, a plaintiff has not suffered a harm that Indiana law is prepared to remedy).

D. Recent Attempts at Reforming Federal Laws Related to Online Data Security

In order to address issues of haphazard data security laws and enforcement actions, various entities including the Obama Administration, Congress, and the FTC have undertaken efforts to guide the U.S. in a direction where such information can be adequately secured through creation of policies such as industry codes of conduct for particular sectors. However, due to concerns from business and community leaders as well as debates among members of Congress, the President and Congress have not worked together to enact comprehensive federal legislation that would pre-empt industry customs in the private sector. These concerns stem from the longstanding belief in the U.S. that it would be better for businesses to regulate themselves than to have government intervene.[78]

1. The Obama Administration's Privacy Framework

In February 2012, the Obama Administration released for the first time a comprehensive privacy framework ("the new framework") to address the evolving issues surrounding the protection of consumer personally identifying information.[79] The new framework recognized that the existing consumer data privacy framework in the U.S. does not effectively deal with consumer data privacy challenges related to personal data shared on the Internet because most federal data privacy statutes apply only to specific sectors.[80] Accordingly, the Obama Administration indicated in its report that it aims to promote more consistent responses to privacy concerns across the wide range of environments in which individuals have access to networked technologies and in which a broad array of companies collect and use personal data by filling the gaps in the existing framework.[81]

The Obama Administration's release of the new privacy framework was quite timely. In the months prior to the report's release, widespread public outcry regarding online consumer privacy protection was prevalent.[82] For example, following the FTC's settlement with Facebook, Facebook

78. *See* Hoang, *supra* note 3, at 817.

79. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter Privacy Framework].

80. *Id.* at 6.

81. *Id.*

82. *See* Sarah Rich, *White House Releases 'Privacy Bill of Rights' for Consumers, Government Technology,* GovTech.com (Feb. 23, 2012), http://www.govtech.com/policy-management/White-House-Releases-Privacy-Bill-of-Rights-for-Consumers.html.

users lamented the company's new Timeline layout that displays users' posts in the distant past.[83] Additionally, consumers complained about Google's announcement that beginning in March 2012 it would compile user profiles based on usage of its various web products.[84] Accordingly, although online privacy protection issues had existed for several years prior to the White House's release of its new privacy framework, the Obama Administration released its framework as a proposed solution to mitigate such issues at a time when community frustrations regarding online privacy protection were at their peak.

The new framework includes a Consumer Privacy Bill of Rights,[85] which sets forth individual rights and corresponding obligations of companies in connection with personal data that are based on U.S.-developed and globally recognized Fair Information Practice Principles.[86] The Consumer Privacy Bill of Rights applies to commercial uses of "personal data."[87] This term refers to any data, including aggregations of data, which is linkable to a specific individual. This definition is similar to the federal government's definition of "personally identifying information": information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.[88] The Obama Administration plans to encourage stakeholders to implement the privacy framework through sector specific codes of conduct and stated in its report that it will work with Congress to enact these rights through privacy legislation.[89]

With respect to personal data, the Consumer Privacy Bill of Rights provides that consumers have a right to: (1) individual control over what personal data companies collect from them and how those companies may use it;[90] (2) transparency in determining privacy and security practices;[91] (3) an expectation that companies will collect, use, and disclose personal data in ways that are consistent with the context in

83. *Id.*
84. *Id.*
85. *Privacy Framework, supra* note 79, at 10.
86. *Id*. at 7.
87. *Id.* at 10.
88. *Id.* at 10.
89. *Id*. at 2–3.
90. *Id.* at 11. For a more in-depth analysis, *see id*. at 11–14.
91. *Id.* at 14–15.

which consumers provide the data;[92] (4) secure and responsible handling of personal data;[93] (5) the ability to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data;[94] (6) reasonable limits on the personal data that companies collect and retain;[95] and (7) the ability to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[96]

The new framework has been supported by prominent individuals, including the FTC Chairman Jon Leibowitz, who said of the agreement in a statement, "[I]t's great to see that companies are stepping up to our challenge to protect privacy so consumers have greater choice and control over how they are tracked online. More needs to be done, but the work they have done so far is very encouraging."[97] Proponents of the new framework note that it "takes advantage of the flexibility of the self-regulatory processes but assures that new codes of conduct are guided by a comprehensive, forward-looking set of privacy principles and that all interested parties such as consumer advocates have a voice in the process."[98]

However, the new framework has also faced opposition from businesses, some of which believe that this approach could incur serious costs for consumers and reduce competitiveness of America's Internet sector.[99] Critics also are weary that the new framework would lead to a considerable increase in government oversight of the Internet and online commerce.[100] Additionally, critics note that one unintended consequence of greater privacy regulation could be higher prices for sites and services that consumers currently enjoy free of charge.[101] According to their logic, data collection and advertising are the fuel that powers the digital economy.[102] By collecting a little information about consumer web-surfing

---

92. *Id.* at 15–19.
93. *Id.* at 19.
94. *Id.* at 19–20.
95. *Id.* at 21.
96. *Id.* at 21–22.
97. Sean Gallagher, *The White House Announces New Privacy "Bill of Rights," Do Not Track Agreement*, Arstechnica (Feb. 22, 2012), http://arstechnica.com/tech-policy/2012/02/white-house-announces-new-privacy-bill-of-rights-do-not-track-agreement/.
98. Elinor Mills, *Obama Unveils Consumer Privacy Bill of Rights*, Cnet (Feb. 22, 2012), http://news.cnet.com/8301-27080_3-57383300-245/obama-unveils-consumer-privacy-bill-of-rights/.
99. Adam Thierer, *The Problem with Obama's "Let's Be More Like Europe" Privacy Plan*, FORBES (Feb. 23, 2012), http://www.forbes.com/sites/adamthierer/2012/02/23/the-problem-with-obamas-lets-be-more-like-europe-privacy-plan/.
100. *Id.*
101. *Id.*
102. *See id*.

interests, online sites can tailor advertisements to consumers' liking, which helps keep online prices low and can use that data to develop new and better services that make consumers' online lives more rewarding.[103]

Finally, critics of the Obama Administration's new framework state that another unintended consequence to consider is how increased privacy controls might lead to greater governmental interference with the Internet more generally.[104] Drawing an analogy to copyright and child safety debates, critics note that top-down directives such as the recent "Stop Online Privacy Act" (SOPA) in those contexts have proved challenging to enforce.[105] Beyond being unworkable, critics claim that such controls can censor much legitimate speech or commerce on the internet.[106]

2. FTC Privacy Commission Report

In March 2012, following the release of the Obama Administration's privacy framework, the FTC released a Final Report ("the Final Report") setting forth the best practices for businesses to protect consumer data and give businesses greater control over the collection, storage, and use of the personal data they collect.[107] In order to address issues of inconsistent data regulation and companies cutting corners with regard to the protection of personally identifying information of consumers, the Final Report emphasized that the FTC is prepared to work with Congress and other stakeholders to craft baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate.[108] The FTC noted that such legislation should provide clear guidelines as well as adequate deterrence "through the availability of civil penalties and other remedies."[109]

While Congress considers such legislation, the FTC staff, over the course of future years, will encourage industries to implement the FTC's final privacy framework by focusing its policymaking efforts in five main areas.[110] First, the FTC will work to develop and implement an effective and easy-to-use Do Not Track System that would provide

103. *See id*.
104. *Id.*
105. *Id.*
106. *Id.*
107. *See Recommendations*, *supra* note 22, at i.
108. *Id.* at 13.
109. *Id.*
110. *Id.*

consumers with tools to convey that they do not want to be tracked.[111] Second, the FTC will work specifically with companies providing mobile services to develop improved privacy protections, such as the development of clear, short, and meaningful disclosures.[112] Third, the Commission will support targeted legislation that would allow consumers access to information about them that is held by a data broker.[113] Fourth, the Commission will work with Internet Service Providers, social media, and other large platforms to explore privacy and other issues related to comprehensive tracking of consumer online activity.[114] Finally, the FTC will participate in the Department of Commerce's project to develop sector-specific codes of conduct and will continue to enforce the FTC Act against companies engaging in deceptive practices, including the failure to abide by self-regulatory programs they opt-into.[115]

As FTC Chairman Jon Leibowitz has stated, many companies have already adopted the FTC's final recommendations for best practices, and if other companies continue to do so, they will be able to "innovate and deliver creative new services that consumers can enjoy without sacrificing their privacy."[116] Critics of the Final Report, however, note that the FTC has not specifically spelled out how to "ensure consumers have meaningful 'choice' to control the collection and use of their information."[117] Critics have noted that the FTC's overall support for industry self-regulation is disappointing, as the FTC "endorses self-regulation and 'notice and choice,' and fails to explain why it has not used its current Section 5 authority to better safeguard the interests of consumers."[118] Moreover, the FTC Commissioner J. Thomas Rosch, who cast the only dissenting vote in a 3-1 decision to approve the Final Report, has stated "regardless which privacy document is adopted, the issue is whether privacy practices are voluntary or federal requirements."[119]

3. Proposed Cybersecurity Information Sharing Act of 2012

Aside from recent efforts by the Obama Administration and the FTC to provide an updated privacy framework related to online data protection,

---

111. *Id.*
112. *Id.*
113. *Id.* at 14.
114. *Id.*
115. *Id.*
116. John Fontana, *FTC Privacy Report Appeals to Congress as Critics Assail Self-Regulation*, ZDNET (Mar. 26, 2012), http://www.zdnet.com/blog/identity/ftc-privacy-report-appeals-to-congress-as-critics-assail-self-regulation/367.
117. *Id.*
118. *Id.*
119. *Id.*

efforts have been made to introduce data security regulation in Congress. The proposed Cybersecurity Information Sharing Act of 2012 ("Cybersecurity Act") was introduced into Congress in February 2012.[120] If enacted, the Cybersecurity Act would provide private entities with the authority to monitor both their own and third party information systems and information that is "stored on, processed by, or transiting such information systems for cybersecurity threats . . . ."[121] The Act would also allow private entities to manage security breach countermeasures[122] on their own information systems as well as on third party information systems to protect both the systems and the information stored on such systems.[123] Additionally, the Act would allow a private entity to disclose lawfully obtained cybersecurity threat indicators to any other private entity.[124] If a private entity receives or discloses a cybersecurity threat indicator, the Act provides that the entity must make reasonable efforts to safeguard its systems, communications, and records from unauthorized access.[125]

---

120. *See* Cybersecurity Information Sharing Act of 2012, S. 2105, 112th Cong. (2d Sess. 2012).

121. The Act requires that the third party lawfully authorize such monitoring before its commencement. *Id.* at §§ 2(1)–(2).

122. "The term 'countermeasures' refers to actions to 'modify or block data packets' associated with online communications, so long as it is done 'with defensive intent' for the purposes of protecting information systems from cybersecurity threats. . . . The limits on 'countermeasures' allowed under this bill have not been established. If this bill passes, it could take judicial interpretation to establish those limits—but only if cases make it to court." *See* Kurt Opsahl & Rainey Reitman, *Frequently Asked Questions About the Liberman-Collins Cyber Security Act*, ELECTRONIC FRONTIER FOUNDATION (May 31, 2012), https://www.eff.org/deeplinks/2012/05/frequently-asked-questions-about-lieberman-collins-cyber-security-act#indicators.

123. Cybersecurity Information Sharing Act of 2012 § 2(3)–(4).

124. *Id.* at § 3(a).

125. *Id.* at § 3(b)(1). The bill defines a "cybersecuirty threat indicator" as information that indicates or describes one or more of eight things: (1) "malicious reconnaissance" which the bill defines as including "anomalous patterns of communication that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat"; (2) a method of defeating a technical control; (3) a technical vulnerability; (4) a method of defeating an operational control; (5) a method of causing a user with legitimate access to an information system of information to "unwittingly enable the defeat of a technical or operational control; (6) malicious cyber command and control; (7) actual or potential harm caused by an incident, including data exfiltrated as a result of subverting a technical control if it is necessary in order to identify or describe a cybersecurity threat; and (8) "any other attirbute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law." *See* Opsahl and Rainey, *supra* note 122.

After months of additional negotiations with privacy and civil liberties groups, Senators from both parties and industry representatives introduced a revised version of the Cybersecurity Act on July 17, 2012[126] ("Revised Act") in a good faith effort to find a common ground with the bill's opponents.[127] The Revised Act required representative owners of critical infrastructure to organize into sector coordinating councils to develop and propose voluntary outcome-based cybersecurity practices.[128] The definition of critical infrastructure is the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Critical infrastructure protection is important because attacks on critical infrastructure could significantly disrupt the functioning of government and businesses alike and produce cascading effects far beyond the targeted sector and location of the incident.[129]

A second main revision to the original bill was the creation of a National Cybersecurity Council, which would be comprised of representatives from the Departments of Commerce, Defense, Homeland Security, Justice, appropriate sector-specific Federal agencies, and other Federal agencies with responsibilities for regulating the security of critical infrastructure.[130] The Revised Act would require the National Cybersecurity Council to institute a voluntary cybersecurity program for critical cyber infrastructure. Under this program, owners of critical infrastructure may self-certify that they satisfy the cybersecurity practices developed under Section 103 of the Revised Act and apply for certification.[131] On August 2, 2012, the Senate voted on the Cybersecurity Act, and although a majority of Senators supported the bill, the vote of 52-46 fell short of the 60 votes needed to invoke cloture,[132] or end the debate on the bill, and accordingly the bill was rendered provisionally dead.[133]

Although the Cybersecurity Act is provisionally dead, its introduction has sparked a great deal of debate in the community and has opened the

---

126. *See* Cybersecurity Act of 2012, S. 3414, 112th Cong. (2d Sess. 2012) [hereinafter Revised Cybersecurity Act of 2012].

127. *Cybersecurity*, U.S. SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS, http://www.hsgac.senate.gov/issues/cybersecurity (last visited Apr. 24, 2013).

128. Revised Cybersecurity Act of 2012 § 103.

129. DEP'T OF HOMELAND SECURITY, NATIONAL INFRASTRUCTURE PROTECTION PLAN 7 (2006), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf.

130. Revised Cybersecurity Act of 2012 §101.

131. *Id.* at § 104.

132. Cloture is the procedure of ending debate in a legislative body and calling for an immediate vote. BLACK'S LAW DICTIONARY 291 (9th ed. 2009).

133. *See Cybersecurity*, *supra* note 127.

channels of communication relating to cybersecurity. Significantly, individuals and corporations remain divided on the bill's merits, particularly with respect to the provision related to the voluntary standards, still strongly opposed by many in the business sector.[134]

Debate over the Revised Act has also extended to the federal government. Senators, non-profit organizations, and federal administrative agencies have articulated views on both sides. For example, President Obama avidly supported the Cybersecurity Act, noting that the Act would make it easier for the government to share threat information so critical-infrastructure companies are better prepared.[135] Other supporters of the Revised Act included the Chairman of the Joint Chiefs of Staff,[136] Microsoft Corporation,[137] the American Civil Liberties Union,[138] and top national security leaders.[139] Support for the Revised Act was primarily based on the fact that it protects America's most urgent need—critical infrastructure systems, and focuses on sharing information, including private user data, between big companies and the government.[140] This is important because facilities such as electricity plants, nuclear power plants, working railways and financial networks must be protected from increasingly sophisticated and dangerous cyber attacks.[141] These facilities

134. *See* Ed O'Keefe & Ellen Nakashima, *Cybersecurity Bill Fails in Senate*, WASH. POST, Aug. 2, 2011, http://www.washingtonpost.com/world/national-security/cybersecurity-bill-fails-in-senate/2012/08/02/gJQADNOOSX_story.html.

135. *Id.*

136. *See* Letter from Martin E. Dempsey, Chairman of Joint Chiefs of Staff, to the Hon. John D. Rockefeller IV, Chairman of the Comm. on Commerce, Sci. & Transp. (Aug. 1, 2012), *available at* http://www.hsgac.senate.gov/download/cybersecurity-support-letter-joint-cheifs-of-staff-chairman.

137. *See* Press Release, Fred Humphries, Statement by Fred Humphries, VP of US Government Affairs, Microsoft Corporation on the Cybersecurity Act of 2012 (July 26, 2012), *available at* http://www.hsgac.senate.gov/download/microsoft-cybersecurity-support-statement.

138. *See* Michelle Richardson, *New Cybersecurity Amendments Unveiled to Address Privacy Concerns*, ACLU (July 19, 2012, 5:28 PM), http://www.aclu.org/ blog/national-security-technology-and-liberty/new-cybersecurity-amendments-unveiled-address-privacy.

139. *See* Letter from National Security Leaders to Sen. Harry Reid & Sen. Mitch McConnell (June 7, 2012), *available at* http://www.hsgac.senate.gov/download/cyber security-support-letter-from-top-national-security-leaders.

140. Dave Aitel, *The Cybersecurity Act of 2012: Are We Smarter Than a Fifth Grader?, Huffington Post*, Aug. 3, 2012, http://www.huffingtonpost.com/dave-aitel/the-cybersecurity-act-of-_b_1737129.html.

141. *Id.*

and networks are not as secure as they should be; cyber attacks against infrastructure are up 1,700% since 2009.[142]

In stark contrast to the support the Revised Act has seen from these entities, the Revised Act has been strongly opposed by some businesses and community leaders. The main issue with the Revised Act in critics' eyes is that its solution is unprecedented.[143] During the debate over the Revised Act, critics raised two main arguments against it.[144] First, business advocates argued that the cost of compliance would create an unfair cost for businesses.[145] Second, business advocates argued that the private industry knows best and government regulation just gets in the way.[146]

E. The Need for Online Data Security Reform

The White House Privacy Framework, the FTC's Privacy Commission Report, and the Cybersecurity Act illuminate the need for reform of U.S. privacy laws in the form of federal legislation that contain specific minimum standards for businesses. Such minimum standards should provide specific rules that address exactly the types of consumer information companies are allowed to collect, and provide a standard for ensuring that such information is adequately protected from hackers within corporate data infrastructures. The different entities' proposals show that reform is needed on the national level, but it is not clear from any of these reports or the proposed legislation how these problems can be resolved, especially since there is so much disagreement among government leaders and business advocates.

Although both the White House Privacy Framework and the FTC's Privacy Commission Report provide general guidelines and state that each entity will work with Congress to enact comprehensive privacy legislation in the future,[147] neither the White House, Congress, nor the FTC have released specific guidelines to address cybersecurity issues and mitigate the potential for future data breaches. Moreover, as technology and corporate marketing strategies within the private sector continue to progress, corporations are increasingly tempted to gather and use consumer information without providing consumers with meaningful disclosures as to what information is being collected. Companies are also tempted

---

142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.*
147. *Privacy Framework*, *supra* note 79, at 2; *Recommendations*, *supra* note 22, at 13.

to gather information without informing consumers about what the corporation will use it for and without obtaining explicit consent for the collection and use of personal information from consumers. In this rapidly advancing area of technology, Congress and the President need to address the aforementioned regulatory issues with respect to online data security, while also respecting the various individual, government, and community interests at stake.

As the Obama Administration noted in its new privacy framework, the existing U.S. privacy framework does not effectively address consumer data privacy challenges related to personal data shared on the Internet.[148] Therefore, the federal government should harmonize its approach to personal data protection with that of other nations or regions that are more successfully protecting data, such as the EU. Doing so would assist the federal government in finding a middle ground in online privacy legislation that would adequately satisfy individual privacy interests, governmental interests, and the interests of large and small businesses.

III. LOOKING BEYOND THE U.S.: THE EU DATA PROTECTION DIRECTIVE

The EU legislates in two ways, through regulations and directives. EU regulations are the most direct form of EU law.[149] As soon as a regulation is passed, it automatically becomes part of the national legal system of each Member State.[150] EU directives, on the other hand, lay down specific end results that must be achieved by each EU member state.[151] Directives are used to bring different national laws in-line with each other.[152] Directives may apply to one or more Member States, or all of them.[153] National authorities must adapt their laws to meet the directive's goals, but are free to decide what laws to implement and how to implement them.[154] Each directive specifies a deadline by which national

148. *Privacy Framework*, *supra* note 79, at 6.
149. Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 815, 823 (2012).
150. *Id.*
151. *See* Secretariat-General, *What Are EU Directives?*, EUROPEAN COMMISSION (Apr. 15, 2013), http://ec.europa.eu/eu_law/introduction/what_directive_en.htm.
152. *Id.*
153. *Id.*
154. *Id.*

authorities must adapt their national laws.[155] Directives are especially common with regard to matters that affect a single market's operation.[156]

A. EU Data Protection Directive 95/46/EC

In the international community, the EU serves as a prominent leader with respect to online data privacy legislation and regulation.[157] Contrary to the U.S. sector-by-sector approach to data protection, the EU approach under Directive 95/46/EC creates a privacy protection program for businesses and consumers that are engaged in the transfer of personal data that is based on "comprehensiveness."[158] The term "comprehensiveness" refers to a broad scheme of privacy standards enforcement, which combines aspects of privacy law across different industries under a single umbrella regime, referred to as "adequate protection" by the EU.[159]

In the 1970s, the growing popularity and use of computers to process personal information created a need for comprehensive data protection legislation.[160] In response, the European Commission ("the Commission") adopted Data Protection Directive 95/46 ("Directive"), which established a comprehensive framework for personal data processing.[161] The Directive has two principal objectives.[162] The first is protecting the fundamental rights of individuals with respect to the processing of personal data,[163] and the second is facilitating the free flow of personal data between EU

---

155. *Id.*

156. Product safety standards provide one example of a matter that affects the operation of a single market. *Id.*

157. 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, 422 (2002).

158. Kamaal Zaidi, *Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 MICH. ST. J. INT'L L. 169, 171 (2003).

159. *Id.*

160. Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, 18 RICH. J.L. & TECH 2, 4 (2011).

161. *Id.* at 4. The Directive's legal authority originates from Article 95 of the European Community Treaty, which allows for the creation of legislation that is aimed at harmonizing the internal market within the EU. *Id.*; *see also* Treaty Establishing the European Community, art. 95, Dec. 29, 2006, 2006 O.J. (C 321E) 37 (consolidated version).

162. *See* Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter *Data Protection Directive*].

163. The right to protection of personal data is now a fundamental right in and of itself in the EU legal system. *See* Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364/1) at art. 8, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf. "Everyone has the right to the protection of personal data concerning him or her." *Id.*; *see also* Consolidated Version of the Treaty on the Functioning of the European Union, 2008 O.J. (C 115/47), at art. 16, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:en:PDF.

Member States.[164] In order to accomplish these aims the Directive sets out a blanket framework for the processing of personal data to be applied to all twenty-seven EU Member States.[165]

The Commission's role with respect to EU directives is to ensure individuals, national authorities, and other EU institutions properly apply EU law.[166] Similar to the FTC's role under the "deceptive practices" prong of the FTC Act, the Commission can impose sanctions on individuals or companies who break EU law.[167] Moreover, like the FTC, the Commission can take formal action against national authorities[168] if the Commission suspects that they are breaking EU law, and can request them to remedy the situation by a certain date.[169] In contrast, the FTC's enforcement work is done through administrative proceedings and in federal court actions.[170]

The Directive applies "to the processing of personal data wholly or partly by automatic means," and to non-automatic processing "of personal data which form part of a filing system or are intended to form part of a filing system."[171] The Directive defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')."[172]

---

164. *Id.* at art. 1. Interpreting the scope of the Directive, the European Court of Justice has determined that Article 1 of the Directive should be read in light of the fact that the object of national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized in Article 8 of the European Convention on Human Rights and Fundamental Freedoms ("EHCR"). *See* Case C-465/00, Rechnungshof v. Österreichischer Rundfunk and Others and Joined Cases C-138/01 and C-139/01 Neukomm and Lauremann v. Österreichischer Rundfunk, 2003 E.C.R. I-4989.

165. Kirsch, *supra* note 160, at 5. The Directive is also incorporated into the 1992 Agreement on the European Economic Area and is therefore also binding on the three European Economic Area European Free Trade Association States, Norway, Iceland, and Liechtenstein. *See generally*, Agreement on the European Economic Area, Mar. 17, 1993, O.J. No. L 1,3.1.1994, p.3, *available at* http://www.efta.int/~/media/Documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEA agreement.pdf.

166. *See* Secretariat-General, *Application of EU Law: The Commission's Role*, EUROPEAN COMMISSION (Apr. 15, 2013), http://ec.europa.eu/eu_law/introduction/what_directive_en.htm.

167. *Id.*

168. Such action may involve bringing an action against them in the European Court of Justice. *Id.*

169. *Id.*

170. *See FTC Actions*, FEDERAL TRADE COMMISSION, (Apr. 15, 2013), http://www.ftc.gov/os/index.shtml.

171. *See* Data Protection Directive, *supra* note 162, at art. 3(1).

172. Data Protection Directive, *supra* note 162, art. at 2(a).

Processing is broadly defined and includes "any operation, or set of operations which is performed upon personal data. . . ."[173] Finally, the definition of a controller encompasses both governmental and private entities, as it is broadly defined to include any natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.[174]

Although the Directive broadly applies to the processing of personal data, the Directive also includes specific exceptions and circumstances in which it does not apply.[175] Moreover, the Directive imposes ex ante controls on data "controllers," setting forth what enterprises must do before they process data.[176] Specifically, the Directive requires controllers to inform the data subject of the "identity of the controller and of his representative (if any)"; the "purposes of the processing for which the data are intended"; and other necessary information to ensure data is fairly processed, including the "recipients or categories of recipients of the data."[177] Furthermore, the data can only be processed and used for the purposes specified.[178] The EU Directive also specifically requires that individuals be informed before personal data are disclosed for the first time to third parties for direct marketing purposes, and be expressly offered the right to object to such disclosures or uses.[179]

Where sensitive information is being collected, such as personal data revealing racial or ethnic origin, political opinions, or data related to health or sex life, the Directive provides that Member States must prohibit processing or require that processing may only occur if the individual has given explicit consent to the processing.[180] Additionally,

---

173. *See* Data Protection Directive, *supra* note 162, at art. 2(b).

174. *See* Data Protection Directive, *supra* note 162, at art. 2(d).

175. The Directive does not apply to processing of personal data in the course of an activity which falls outside the scope of Community law, such as in cases where processing operations concern public security, defense, State security, activities of the State in areas of criminal law, and in cases where processing operations are done by a natural person in the course of a purely personal or household activity. *See* Data Protection Directive, *supra* note 162, at art. 3(2), 6(1), 13.

176. Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Racheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 13 (2000).

177. *See* Data Protection Directive, *supra* note 162, at art. 10.

178. *See* Data Protection Direcitve, *supra* note 162, at art. 6. Article 6(1)(b) states that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." *Id*. at art. 6(1)(b).

179. *See* Data Protection Directive, *supra* note 162, at art. 14(b).

180. *See* Data Protection Directive, *supra* note 162, at art. 8(1)–(2). The Directive's prohibition, however, is subject to limited exceptions set forth in article 8(2)(a)–(e), the most important of which is set forth in article 8(2)(a), which states that "Paragraph 1 shall not apply where: the data subject has given his explicit consent to the processing of

the Directive imposes ex post controls on enterprises, granting individuals rights to monitor and dispute the use of personal information after it is processed.[181] Finally, the Directive requires Member States to "provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question," which includes the right to damages.[182] As for liability, the Directive provides that a controller may be exempt from liability if "he proves that he is not responsible for the damage."[183] Therefore, the controller has the burden to disprove liability.[184]

One of the most frequently quoted positive aspects of the Directive has been its impact in sparking a debate on the subject of data protection.[185] The Directive can be credited with formulating legally binding rules that are effective law across the Member States with regard to automatic processing of personal data.[186] As a result, the Directive garners international respect, and its principles exemplify a standard for good data protection practices even in contexts where it does not directly apply.[187]

To a large extent, the Directive does not address the way in which its provisions should be applied in specific sectors, such as the health or financial services sectors, or in the context of new technologies.[188] Personal data has deliberately been defined abstractly so that it can be applied in numerous technological contexts.[189] The definition relies on considerations of 'content,' 'purpose' and 'result,' and can therefore be applied to behavioral data, biometric data, or characteristics that a data controller may assign, such as a passport or driver's license number.[190] Therefore, the legal framework is not restricted to a specific technological

---

those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent." *See* Data Protection Directive, *supra* note 162, at art. 8(2)(a) (emphasis added).

181. *See* Shaffer, *supra* note 176, at 16.

182. *See* Data Protection Directive, *supra* note 162, at art. 22–23.

183. European Union Data Protection, INT'L QUARTERLY (Thomson Reuters), Jan. 2008, at (I)(B).

184. *Id.*

185. NEIL ROBINSON, HANS GRAUX, MAARTEN BOTTERMAN & LORENZO VALERI, RAND EUROPE, REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 22 (2009), *available at* http://www.rand.org/pubs/technical_reports/TR710.html (Click "Click to Read Online").

186. *Id.*

187. *Id.*

188. *Id.* at 24.

189. *Id.*

190. *Id.*

or societal context, so national data protection authorities can elucidate how the Directive's provisions should apply in each context, if necessary.[191]

Some criticize the Directive's scope, however, because there is no clear definition of the nexus between privacy protection and data protection, and there is no clear privacy impact on all acts of personal data processing that the Directive addresses.[192] The basis of the Directive's approach is the two main objectives of protecting the right of privacy and preventing barriers to allowing information to flow freely within the European Union.[193] However, the concept of personal data is very broad and subject to much debate.[194] Some argue that any potential link of data to a specific individual should be personal data.[195] That interpretation views Internet Protocol (IP) addresses as personal data even if there is uncertainty as to whether the data processing entity can connect it to a specific individual.[196] Dealing with large sets of anonymized data is also challenging.[197] In the healthcare arena, for example, researchers use large sets of clinical data that is de-personalized to make the information as anonymous as possible for statistical analysis.[198] However, regardless of how thoroughly the data is de-personalized, under an absolute interpretation it is still categorized as personal data if there is a possibility of connecting the data to a particular individual, however remote or complex that may be.[199]

A relative interpretation of personal data notes that, in order to find that data "relate" to an individual, either a "content," a "purpose," or a "result" element should exist.[200] This interpretation defines data as personal data when the data includes information about a specific person (content); when the data is used or likely to be used to determine how a specific person will be treated (purpose); or when the data is likely to impact a

---

191. *Id.*
192. *Id.* at 27.
193. James R. Maxeiner, *Freedom of Information and the EU Data Protection Directive*, 48 FED. COMM. L.J. 93, 96 (1995).
194. ROBINSON, *supra* note 185, at 27.
195. *Id.*
196. *Id.*
197. *Id.* Recital 26 in the preamble to the Directive states that, "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable." *See* Data Protection Direcitve, *supra* note 162, at pmbl. (26).
198. *Id.*
199. *Id.* Such an absolute interpretation, however, does not take into account the fact that recital 26 in the preamble to the Directive states that, "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." *See* Data Protection Directive, *supra* note 162, at pmbl. (26).
200. ROBINSON, *supra* note 185, at 27.

specific person in some way (result).[201] Therefore, this interpretation does not always allow the classification of IP addresses or user names as personal data, and the context within which the data is processed determines whether the data meet the "content," "result," or "purpose" criteria.[202] Defining "personal data" is particularly challenging in the context of mobile communications.[203]

At present, the EU is in the process of revising the Data Protection Directive.[204] One major reason for the revision is the non-uniform implementation by EU member states of the definition of informed and free consent.[205] "On November 4, 2010, the European Commission explained that challenges with respect to personal data protection had arisen over past decades which created a need to update the original Data Protection Directive.[206] These challenges include the threat posed by new and increasingly sophisticated forms of collecting and analyzing personal data that allow companies to more effectively target consumers based on their online shopping and browsing behavior.[207]

B. Draft European Data Protection Regulation

On January 25, 2012, the European Commission unveiled a proposed data protection package that set out new enforcement powers for privacy agencies.[208] The Commission's goal in creating the Draft European Data Protection Regulation ("Draft Regulation") was to build a "stronger, more coherent data protection framework" backed by strong enforcement to allow the digital economy to develop further across the internal market.[209] Moreover, the new Draft Regulation would place individual consumers

201. *Id.*
202. *Id.*
203. *Id.*
204. *See* Kirsch, *supra* note 160, at 7.
205. *Id.*
206. *Id.* at 22.
207. *Id.*
208. *See generally Proposal for a Regulation of the European Parliament and Of the Coucil on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, EUROPEAN COMMISSION Jan. 25, 2012, *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter Draft Data Protection Regulation].
209. *Id.* at 2.

in control of their own data and would bring consistency and certainty to economic operators and public authorities.[210]

Rather than issuing another directive similar to the Data Protection Directive 95/46/EC, the Commission adopted a new framework for data protection based on a bilateral approach whereby a Regulation ("Proposed Regulation") would deal with general privacy issues and a Directive ("proposed directive") would focus on issues relating to criminal investigations.[211] The fact that the Proposed Regulation and Proposed Directive have been published indicate the potential for a significant change in the way data protection is addressed in the future throughout the EU.[212] If the Proposed Regulation and Proposed Directive are adopted, EU member states will, for the most part, function under a single data protection law that is directly applicable to all entities and individuals.[213]

One of the most significant changes EU member states would be required to adapt to if the Proposed Regulation is adopted is the altering of the consent process to require that there be "explicit" consent from the data subject.[214] This may be given by an individual data subject in several ways: (1) the individual's statement of consent; (2) a clear, affirmative action by the individual that demonstrates to the processor that he is aware and provides his consent to the processing of his personal data, such as selecting a box when visiting a website; or (3) any other statement or action by the individual which clearly indicates his acceptance of the proposed processing within the specific context.[215] Additionally, the Proposed Regulation also adds new concepts such as the protection of individual information of children, the concept of a security breach, and the use of binding corporate rules, none of which were included in Directive 95/46/EC.[216]

In its efforts to provide for harmonization of data privacy laws across the Member States, the Proposed Regulation also includes several modifications to bridge the gaps in Directive 95/46/EC. For example, the Proposed Regulation provides for a data subject's right to be forgotten and to erasure.[217] Additionally, it provides a more specific definition of the "right of erasure" included in Article 12(b) of Directive 95/46/EC and defines specific conditions of the right to be forgotten.[218] As defined

---

210. *Id.*
211. Gilbert, *supra* note 149, at 815–16.
212. *Id.* at 816.
213. *Id.* at 816–17.
214. *Id.* at 826.
215. *See* Draft Data Protection Regulation, *supra* note 208, at 21.
216. Gilbert, *supra* note 149, at 826.
217. Draft Data Protection Regulation, *supra* note 208, at 9.
218. *Id.*

by the Proposed Regulation, if the data must be removed either at the request of the data subject or due to non-compliance on the part of the controller, the controller must take all reasonable steps to notify third parties which are processing the data that they must remove any access to that personal data and must not copy or replicate the data.[219] Moreover, in situations where the controller has allowed a third party to publish the data, the controller will be held responsible for the publication.[220]

Additionally, the Proposed Regulation would create a "mandatory data protection officer" position both in the public sector and for large entities in the private sector where the controller's primary responsibilities are focused on processing operations "requiring regular and systematic monitoring."[221] Furthermore, under the Proposed Regulation, the controller and processor of the data would be required to assign a data protection officer in cases where the processing is done by a public authority, or by an enterprise employing 250 persons or more.[222]

The Proposed Regulation provides that the controller or processor is required to designate the data protection officer on the basis of professional qualifications, and specifically requires that the officer have "expert knowledge of data protection law and practices and ability" to execute its tasks.[223] With such expert knowledge, the data protection officer would, among other things, be put to the tasks of informing and advising the controller of his obligations pursuant to the Proposed Regulation, to monitor the controller's implementation and application of the policies related to personal data protection, including training staff involved in processing operations, and monitor the requirements of the Proposed Regulation.[224]

In addition to designating a data protection officer and laying out the data protection officer's tasks, the Proposed Regulation also addresses codes of conduct and certification.[225] According to the Proposed Regulation,

---

219. *Id.* at 51.
220. *Id.*
221. *Id.* at 11.
222. *Id.* at 65.
223. *Id.*
224. *Id.* at 66.
225. *Id.* at 67. Data Protection Directive 95/46/EC also encourages "the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States," however, the Proposed Regulation provides more specific criteria Member States should take into account when encouraging development of such codes of conduct. *See* Data Protection Directive, *supra* note 162, at art. 27.

Member States should encourage the development of codes of conduct, "taking into account the specific features of various data processing sectors," and in particular with respect to the collection of data, transparent data processing, information of both the general public and specific data subjects, and the transfer of data to third countries or international entities.[226] Under the Proposed Regulation, associations or other entities representing categories of controllers or processors in one Member State must submit proposed codes of conduct to the Member State's supervisory authority, which will then provide an opinion on whether the draft code of conduct is in compliance with the Proposed Regulation.[227]

Finally, the Proposed Regulation sets out mandatory obligations for any transfer of personal data to third countries or international organizations.[228] Building on Article 25 of Directive 95/46/EC, the Proposed Regulation sets out criteria, conditions, and procedures for the Commission's adoption of an adequacy decision, and establishes that a transfer may only take place where the Commission already decided that the third country ensures an adequate level of protection.[229]

The Proposed Regulation lays out several elements the Commission should consider when assessing the adequacy of the level of protection.[230] These elements include: the applicable rule of law, professional rules and security measures the specific country abides by, and the judicial redress available for individuals whose personal data are being transferred within the Union.[231] Additionally, the Commission considers the existence and effective functioning of one or more independent supervisory authorities in the third country or international organization responsible for ensuring compliance with the data protection rules.[232] Finally, the Commission must consider any international commitments the third country or international organization has entered into.[233]

---

226. The Proposed Regulation also provides that Member States, supervisory authorities, and the Commission should also heavily take into account: "the information and protection of children; mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it; [and] out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respec to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75." Draft Data Protection Regulation, *supra* note 208, at 67.

227. *Id.* at 67–68.

228. *Id.* at 11.

229. *Id.* at 69.

230. *Id.* at 69.

231. *Id.*

232. *Id.*

233. *Id.*

IV. RECOMMENDATION: HARMONIZATION OF U.S. LAWS WITH THE EU'S APPROACH

To solve the problem of inconsistent online privacy regulation in the U.S., the federal government must work together with key leaders in the business community to reform U.S. data protection laws. First, the President, Congress, and the FTC must work together to pass uniform federal legislation that would set a minimum nationwide privacy standard for entities within the public and private sectors by harmonizing the U.S. approach with the EU's approach of, at a minimum, providing broad principles to govern online data privacy. The U.S. should follow in the footsteps of the EU model and institute a data controller within both the public and private sectors in order to control the collection and dissemination of online personal information of consumers. Second, federal legislation should fall in line with the EU's current Data Protection Directive 95/46/EC and require both public and private entities to provide transparent, meaningful disclosures to consumers regarding the purposes for which the entities collect their personal information. Additionally, the federal government should follow the EU's movement, seen in the Proposed Regulation, toward allowing consumers to have a "right to be forgotten" and to "erasure" that would, upon the consumer's request, mandate corporations to stop tracking the data subject's information and instruct any third parties to destroy any information obtained from that data subject.

Finally, the FTC should work with industry leaders within the business communities to follow through on its plans to implement industry specific codes of conduct that businesses can opt into by self-certifying their compliance with such codes of conduct. In doing so, the FTC should take into account the types of minimum requirements required of companies in enforcement action settlement agreements, such as those addressed in the Facebook enforcement action as a starting point for discussion within the business communities. As a result, this approach may serve as a model for solving future online data security issues.

A. Setting a Minimum Nationwide Privacy Standard

The President, Congress, and the FTC should work together to pass legislation that would set a minimum nationwide privacy standard for entities within the public and private sectors. Specifically, the U.S. should

use the EU Data Protection Directive 95/46/EC as a guide. Advantages of the Directive include structural aspects necessary for any successful data processing system, which the legislature should reference as a starting point.[234] Like the EU model, the U.S. should consider passing legislation that mandates that, at a very minimum, information collected from data subjects must be processed fairly and lawfully; collected for specific, explicit and legitimate purposes; and must be accurate and kept up to date.[235]

Furthermore, legislation should provide that entities store data in a form that allows identification of data subjects for a period no longer than is necessary for the purposes for which the entities collected the information.[236] In order to streamline this process, the federal government should consider the provisions currently under consideration within the EU's Proposed Regulation. These provisions would implement data protection officers in the public and private sectors for processing operations that require regular and systematic monitoring and specifically where the processing is carried out by a public authority or body; or is carried out by an enterprise employing 250 persons or more.[237]

B. Requiring Meaningful Disclosures from Data Controllers

Additionally, the U.S. should use the EU model for guidance regarding the types of disclosures that must be made to data subjects when their personal information is being collected. New disclosure legislation should require, at a minimum, that controllers of the data provide the data subject with the following information: (1) the identity of the controller and of his representative, if any; (2) the purposes of the processing for which the data are intended; (3) any other information, such as the recipients or categories of recipients of the data; (4) and the existence of the right of access to and the right to rectify the data concerning him.[238] Enacting these requirements for entities within the public and private sector would create greater awareness among individuals regarding the exact type of information gathered. They would also provide several points of contact for the data subject in the event of a security breach or a concern about collection of certain personal information.

---

234. *See* Nicole M. Buba, *Waging War Against Identity Theft: Should the United States Borrow From the European Union's Batalion?*, 23 SUFFOLK TRANSNAT'L L. REV. 633, 656 (2000).
235. *See* Data Protection Directive, *supra* note 162, at art. 6.
236. *Id.*
237. *See* Draft Data Protection Regulation, *supra* note 208, at 11 (summarizing Article 35 of the Draft Data Regulation).
238. *See* Border, *supra* note 8, at 374.

Moreover, such disclosures would help plaintiffs like those in *Reilly* and *Krottner* to establish standing in federal data breach cases because such disclosures would require corporations to monitor and affirmatively document the specific data collected and the release of the data to specific individuals. This is because such disclosures would require public and private entities to streamline their data infrastructure policies, leading to more stringent monitoring of access to information systems by hackers.

C. Requiring Data Controllers to Obtain Affirmative Consent from Consumer Data Subjects

Furthermore, in addition to requiring data controllers to provide data subjects with such disclosures, the U.S. should use the EU's January 25, 2012 Proposed Draft Data Protection Regulation as a model to start a discussion regarding imposition of a requirement of explicit, affirmative consent from data subjects. Under current U.S. data security regulation, many corporations that operate solely within the online marketplace do not provide meaningful disclosures to consumers. These companies often begin tracking user data or allowing third party access to user information that the data subject is completely unaware of and did not consent to, as was the case in the Facebook enforcement action. To combat this, at the very minimum, both public sector agencies and companies within the private sector should be required to obtain clear, affirmative consent from the data subject, ensuring that the individual is aware that he gives his consent to the processing of personal data, and silence or inactivity should not constitute consent on the data subject's part.[239]

Requiring consumers to affirmatively, explicitly consent to data collection and tracking policies would create an affirmative obligation on the part of companies. "Affirmative consent" occurs when the consumer must take action, such as checking a box that states "I agree," before a company adds the consumer to an e-mail list or sends promotional materials based on the consumer's web browsing activity.[240] Some community leaders and commentators recommend companies enact best practices, such as including a link in their privacy statement at the point

239. *See* Draft Data Protection Regulation, *supra* note 208, at 21.

240. *See, e.g.*, *Direct Marketing Association's Online Marketing Guidelines and Do the Right Thing Commentary*, DIRECT MARKETING ASSOCIATION, http://www.the-dma.org/guidelines/onlineguidelines.shtml (last visited Apr. 24, 2013).

of collection of an e-mail address, as well as each subsequent e-mail, for easy access to the enterprise's privacy notice.[241]

Additionally, commentators encourage enterprises to include references within the consumer's first e-mail message to remind consumers how the enterprise obtained their e-mail address, what they signed up for, and why they are receiving an e-mail.[242] When using a third party list, the enterprise's solicitation should identify the source to remind consumers of where and when they granted permission.[243] Finally, commentators recommend that in each solicitation sent online, marketers should provide individuals with a link or notice they can use to request that the marketer remove them from future solicitations online, and request that the marketer not rent, sell, or exchange their e-mail addresses for online solicitation purposes.[244]

D. Allowing Consumers to Opt-Out of Data Collection Policies

Finally, in addition to requiring agencies and private entities to obtain affirmative consent before tracking consumers, federal legislation should also adopt the EU Proposed Regulation's model of providing for an individual's "right to be forgotten" and to "erasure" that would, upon a data subject's request, mandate corporations to stop tracking the subject's information and instruct third parties to destroy any information obtained from the data subject.[245] Requiring such action upon the affirmative statement of the data subject would provide individuals the opportunity to play an active role within the data collection process.

The legislature will undoubtedly face several challenges from the business community when considering implementing a broad federal regulation, as it has seen with the proposed Cybersecurity Information Sharing Act of 2012. Many businesses and members of the electronic commerce community continue to remain opposed to statutory regulations because they believe in industry self-regulation.[246] Successful statutory guidelines, therefore, must combine aspects important to both consumers, concerned with personal privacy, and industry participants, who are concerned with economic profit and the uninhibited free flow of data.[247]

---

241. *Id.*
242. *Id.*
243. *Id.*
244. *Id.*
245. *See* Draft Data Protection Regulation, *supra* note 208, at 9.
246. *See* Buba, *supra* note 234, at 659–60.
247. *Id.* at 660.

E. FTC Development of Industry Codes of Conduct

In addition to developing broad federal legislation regarding online data security, the FTC should work with industry leaders within prominent business communities to follow through on its plans to implement voluntary industry specific codes of conduct relating to data security. Like any drafted federal legislation, industry specific codes of conduct should balance the privacy interests of individuals with the interests of industry participants in the uninhibited free flow of data. Accordingly, the legislature and the FTC should work to establish broad standards for online data protection that apply across industries and disciplines.

Once the creation of such industry codes of conduct occurs, businesses may have the option to voluntarily self-certify their compliance with such codes and FTC recommendations. Allowing business advocates the choice to self-certify compliance with the codes of conduct for respective sectors (e.g. financial services or social networking services) would allow businesses greater choice and influence within the development process. Furthermore, if companies that self-certify to specific industry codes of conduct fail to follow them or seek to cut corners by failing to adhere to all parts of the relevant code, the FTC can then use its enforcement authority under the Deceptive Practices prong of the FTC Act to impose fines or sanctions on the company. FTC enforced consequences would ensure that companies face adequate legal barriers to cutting corners or to voluntarily self-certifying to industry codes when in fact they do not intend to abide by the code.

1. Right to be Forgotten

The Obama Administration's Privacy Framework provides an excellent starting point for developing industry codes of conduct because it establishes minimum standards for all industries in relation to online data security. First, the FTC should mandate that industry specific codes require private companies to make their privacy and security practices transparent to citizens.[248] This standard would require collectors of personal information to give individuals notice for the collection of personal

248. *Privacy Framework*, *supra* note 79, at 14–15.

information, and even potentially require affirmative consent from individuals for certain processing and use of personal information.[249]

2. Requirement that Enterprises Engage in Secure and Responsible Handling of Online Consumer Data

Second, industry specific codes of conduct should require the secure and responsible handling of personal data, and establish greater scrutiny and protection for sensitive information including data pertaining to characteristics such as race, religion, health, or political beliefs.[250] Next, industry codes should allow individual data subjects access to the personal data collected, and offer them the ability to correct their personal data in a manner appropriate to the sensitivity of the data.[251] Finally, the FTC should work with industry and key community business leaders to place reasonable limits on the types of personal information companies collect and retain.[252]

Although the FTC will certainly face challenges from business leaders and must, therefore, exercise caution and avoid overstepping its authority when approaching industry leaders, the government has seen progress. The President, Congress, and the FTC made strides with business leaders by releasing proposed legislation and reports such as the Obama Administration's Privacy Framework and the FTC Privacy Commission Report. At this point, the legislature is in an ideal position to open the door to further discussions regarding data security protocols within the private sector. Additionally, the FTC's recent aggressive enforcement efforts on companies such as Facebook and Google provide added incentive for companies within the private sector to work with the FTC.

V. CONCLUSION

Data protection laws continue to change with the times and the invention of new technology. Therefore, it is imperative for the federal government to set out clear guidelines related to cyber security and data protection. Although the FTC and the Obama Administration set forth privacy frameworks, these frameworks merely provide recommendations to legislators and individuals within the business community for implementing data security procedures. Such broad frameworks have caused confusion in the national community with regard to what standards to follow. Thus,

---

249. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 515 (1995).
250. *See id.*
251. *Privacy Framework*, *supra* note 79, at 19–20.
252. *Id.* at 21.

creating uniform baseline rules through federal legislation that sets a minimum standard, but provides for both industries and states to implement their own respective codes of conduct that address data protection, serves as the best approach to resolving the debate on data security in the future.