Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix it

Bradyn Fairclough

I. INTRODUCTION

2015 was an unkind year to people who cheat. A group of hackers obtained and threatened to leak gigabytes of personal information of the users of Ashley Madison,[1] a website used by individuals seeking to have an extramarital relationship, if the site was not shut down immediately.[2] To the humiliation of thousands of users, the hacker group leaked names, sexual fantasies, credit card information, addresses, and more.[3]

The news was frightening for many because of Ashley Madison's practice of never deleting their users' private information.[4] However, injuries stemming from data breaches do not only affect the unsympathetic. Simply shopping at Target put 40 million credit and debit card accounts in jeopardy when the company announced that they had been the victim of a data leak in 2013.[5]

Even more troubling to some is not just that companies are not adequately protecting against incidents of data leakage, but that these companies will often leak the information on purpose.[6] Many websites use up to 100 tools to track consumer data.[7] Companies will often sell a consumer's location, age, and other personal details to "data brokers," who in turn distribute this information to third parties.[8] Not only are these facts shocking to some, it is even more shocking that businesses in the United States actually have a large role in creating the rules that regulate their actions.[9]

The data leaks at Ashley Madison, Target, and many other companies suggest that consumer protection requirements for businesses are not stringent enough. This Note will discuss the United States's data privacy problem and some solutions scholars have proposed to affect widespread compliance by businesses and protection for consumers. Part II will discuss the history of data privacy in the United States and in the European Union (EU). Part III will analyze proposed solutions to the U.S. privacy problem and discuss their viability. Part IV will recommend a solution that the United States can implement to provide more protections to its citizens without damaging its growing data-driven economy.

---

1. ASHLEY MADISON, https://www.ashleymadison.com (last visited Oct. 25, 2016).

2. Simon Thomsen, *Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online*, BUS. INSIDER (July 20, 2015, 4:31 AM), http://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7.

3. Brian Krebs, *Online Cheating Site AshleyMadison Hacked*, KREBSONSECURITY (July 19, 2015), https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked.

4. Thomsen, *supra* note 2.

5. Charles Leaver, *Millions of Target customers affected by data leakage*, ZIFTEN (Dec. 20, 2013), http://ziften.com/millions-of-target-customers-affected-by-data-leakage/.

6. *See* Bonnie Lowenthal, *Right to Know Act (AB 1291)*, AM. CIV. LIBERTIES UNION OF N. CAL., https://www.aclunc.org/our-work/legislation/right-know-act-ab-1291 (last visited Oct. 25, 2016) (noting that apps will share "location, age, gender, phone numbers, and other personal details . . . with third party companies").

7. *Id.*

8. *Id.*

9. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, https://build.export.gov/main/safeharbor/eu/eg_main_018476 (last updated Dec. 18, 2013, 3:45 PM) (describing how the U.S. data privacy regime relies in part on "self-regulation," specifically industry standards, codes of conduct, and the current marketplace) [hereinafter *U.S.–EU Safe Harbor*].

II. BACKGROUND: AN OVERVIEW OF THE U.S. MODEL AND THE EU MODEL

Modern-day data privacy laws protecting private information in the United States and the EU grew out of the 1970s Fair Information Practice Principles (FIPPs).[10] The FIPPs outline eight essential pillars of effective data security: 1) transparency, 2) purpose specification, 3) use limitation, 4) data minimization, 5) data accuracy, 6) individual participation, 7) security, and 8) accountability.[11] Although the United States developed the principles, the country has not yet fully embraced them; instead, the United States relies on a fractured system comprised of various acts and statutes that did not begin with a glance at the FIPPs, but rather grew out of what each industry individually needed.[12] The EU, however, has made a conscious effort to incorporate the FIPPs into its Data Directive; the Data Directive is widely recognized globally as providing more protection for consumers' private information than the EU's regulations.[13] This Part will discuss the data protection models that both the United States and the EU adopted.

A. The U.S. Model: Criticisms

The United States utilizes a "sectoral model" to regulate how businesses use private consumer information.[14] A sectoral model utilizes legislation, regulation, and self-regulation.[15] Essentially, the sectoral model works like this: Congress passes narrowly tailored laws that barely infringe on the marketplace's role of self-regulation, and the Federal Trade Commission (FTC) and the Department of Commerce monitor businesses relying primarily on industry standards.[16] By partially relying on self-regulation, businesses are expected to abide by intangible industry practices and unwritten codes of conduct that they themselves create and interpret.[17] The sectoral model is used for several reasons. For one, supporters of the model claim that businesses are in the best position to decide what regulations are best for them and their consumers.[18] In addition, another policy reason for this model is that it helps the economy, especially today, as the economy has

10. Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 357 (2015).

11. U.S. DEP'T HOMELAND SEC., MEMORANDUM NO. 2008-01 PRIVACY POLICY GUIDANCE MEMORANDUM (2008), at 1, https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf; *see generally* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (July 1973), http://www.justice.gov/opcl/docs/rec-com-rights.pdf (discussing the impact of computers on data security).

12. *See infra* Section II.A.3 (discussing laws protecting privacy of information); 15 U.S.C. § 45 (2015) (Section Five of the FTC Act) (discussing methods to prevent unfair competition); 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. JUDICIARY 810, 814 (2012) (discussing how laws have been aimed at different sectors); *U.S.–EU Safe Harbor*, *supra* note 9 ("The Priciples were developed in consultation with the industry and the general public to facilitate trade and commerce between the United States and European Union.").

13. Brookman, *supra* note 10, at 357–58.

14. Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada*, *and Europe*, 29 CONN. J. INT'L L. 257, 260 (2014). Conversely, the other model is the omnibus approach, which is broader and involves far-reaching regulations often encompassing both the private and public sectors. *Id.*

15. *U.S.–E.U. Safe Harbor*, *supra* note 9.

16. Hoang, *supra* note 12, at 814.

17. *Id.*

18. *Id.* at 814–15.

become more data-driven.[19] Although businesses have become more data-driven and tech savvy over time, there is one thing that will always drive businesses: profits.[20]

Many have criticized the self-regulated model as being ineffective and laden with conflicts of interest because it asks businesses to regulate themselves when loose regulation could mean a much larger profit.[21] The government has developed laws to regulate the use of private information, but they are often industry-specific and the government applies them narrowly.[22] Businesses ultimately decide how the laws should be implemented in their day-to-day operations.[23] To further complicate the issue, the court system then interprets these laws, resulting in varied outcomes.[24] To illustrate this inconsistency between the courts and what a private citizen might believe is protected by law, it is instructive to note that a Pennsylvania court recently held there is no "common law duty to protect and safeguard confidential information."[25]

The U.S. government is also concerned about infringing on the marketplace and burdening the country's increasingly data-driven economy with over-invasive regulation.[26] President Obama called for action to provide stricter regulation[27] and met considerable opposition, especially in a report decrying any benefits of overarching regulation similar to the EU model.[28] The president even revised his plan and proposed a bill, stressing the new regulation would not burden the economy, but Congress again opposed the bill with

19. Brookman, *supra* note 10, at 361; *see* James Bailey & Diana Thomas, *Red Tape Kills Jobs*, U.S. NEWS (Sept. 14, 2015, 12:15 PM), http://www.usnews.com/opinion/economic-intelligence/2015/09/14/regulations-kill-jobs-data-show (sharing research that suggests regulation in general hurts the economy and stalls job growth).

20. Jason Morris & Ed Lavandera, *Why big companies buy, sell your data*, CNN (Aug. 23, 2012, 3:52 PM), http://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/.

21. Ryan Moshell, *. . . And Then There was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH. L. REV. 357, 367 (2005); Hoang, *supra* note 12, at 848 ("On one hand, businesses are delegated the duty of protecting customer information. On the other hand, businesses need to make a profit, and selling information is very lucrative.").

22. Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1181 (2014).

23. Hoang, *supra* note 12, at 818.

24. *See* Brookman, *supra* note 10, at 364–66 (describing cases brought by the Federal Trade Commission (FTC) under Section Five of the Federal Trade Commission Act).

25. Dittman v. UPMC, No. GD-14-003285, 2015 WL 4945713, at *5 (Pa. Ct. Comm. Pl. May 28, 2015); *see* Steven L. Caponi, *Data Breach Negligence Claims Not Recognized in Pennsylvania*, 27 No. 10 INTELL. PROP. & TECH. L.J. 22, 22 (2015) (discussing the ruling in *Dittman*).

26. *See Internet Privacy: The Impact and Burden of EU Regulation: Hearing Before the Subcomm. on Com., Mfg., & Trade of the H. Comm. on Energy and Com.*, 112th Cong. 52 (2011), https://babel.hathitrust.org/cgi/pt?id=umn.31951d03502152z (finding that the necessary privacy framework is already in place in the Safe Harbor Agreement, that the "directive imposes . . . requirements on companies that often do little to advance privacy protections but that place significant burdens on companies," and that the EU's Directive is fractured and does not take into account the "global nature" of data); William J. Clinton & Albert Gore, Jr., *A Framework For Global Electronic Commerce*, W3C (1997), http://www.w3.org/TR/NOTE-framework-970706 (arguing the private sector should take the reins, and government should avoid burdensome restrictions).

27. *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("With this Consumer Privacy Bill of Rights, we offer to the world a dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies.").

28. *See generally Internet Privacy*, *supra* note 26 (describing the great burdens and few benefits of enacting regulations similar to those used in the EU).

new criticisms that the proposed protections were too weak.[29]

In fact, this cycle has been repeated several times before.[30] Congress or the president will feel that industry practices relating to data security are lacking and begin to threaten and propose stricter legislation.[31] Businesses will respond by purporting to implement stricter policies, pacifying Capitol Hill.[32] Then, as time passes, businesses will shy away from their self-made regulations and the cycle starts all over again.[33]

There is a constant tension between free information, profits, and consumer protection.[34] For example, some new proposed government regulation has required default opt-out policies for the collection and use of information instead of the default opt-in policies that companies use now.[35] On the other side, many argue that increased government regulation and constant pop-ups[36] requesting consumers to opt-in could spell the end of "free internet" and severely hamper many businesses' valuable revenue streams from advertising.[37] There have also been other legal roadblocks to increased data privacy.

1. Constitutional Barriers to Protection

The Constitution and the courts have also not helped data privacy laws progress in the United States.[38] The U.S. Constitution does not contain an explicit right to privacy, but rather those rights are implied in certain areas.[39] Rather than being based in the firm footing

29. Brookman, *supra* note 10, at 361.

30. *Id.* at 362.

31. *Id.* at 362–63. This trend can be seen in at least two instances. One example is in the early 2000s, the advertising industry felt pressure from the FTC to regulate more effectively, so they developed the National Advertising Initiative (NAI) to better self-regulate. *Id.* The NAI was slow to make a change, and within a few years, only two companies were adhering to the new rules. *Id.* Another example occurred in 2012, where the Obama administration pushed privacy legislation for businesses to honor "Do Not Track" flags. Brookman, *supra* note 10, at 362–63. This effort also failed, and only a few companies continue to abide by it. *Id.*

32. *Id.*

33. *Id.*

34. *See supra* Part II.A (explaining some of the criticisms of the U.S. self-regulated model that are behind the tension).

35. *See* Kelsey Maxwell, *Online Behavioral Advertising: The Pros and Cons of Regulation and Suggestions for Adherence to California's Constitutional Right to Privacy*, 19 NEXUS: CHAPMAN'S J.L. & POL'Y 51, 69 (2013–2014) ("Currently, companies operate on a default opt-in policy for collecting and sharing non-personally identifiable information."). "Opt-out" policies require the consumer to take action to prevent a business from sharing their information with third parties or tracking their data. Conversely, "opt-in" policies' default setting is that the business cannot share the consumer's information without the consumer being fully informed and "opting in" to any information sharing. Office of the CISO, *Brief: Opt In Versus Opt Out*, WASH. U. 1–2 (May 2013), https://ciso.uw.edu/site/files/opt_in_opt_out.pdf.

36. These pop-ups, or "click throughs," provide terms of use for information sharing that the consumer can read and then accept or decline. Office of the CISO, *supra* note 35, at 2.

37. *See* Eric Wheeler, *How 'Do Not Track' is poised to kill online growth*, CNET (Sept. 20, 2012, 4:07 AM), http://www.cnet.com/news/how-do-not-track-is-poised-to-kill-online-growth/ (discussing the multi-billion dollar industry of online advertising, the millions of consumers that have already opted out under already strict standards, and the possibly dire implications of further restrictions for start-ups and small businesses).

38. *See infra* notes 39–45 (describing the progression of data laws in the United States).

39. Roe v. Wade, 410 U.S. 113, 152 (1973) ("[T]he Court has recognized that a right of personal privacy, or a guarantee of *certain areas or zones of privacy*, does exist under the Constitution. In varying contexts, the Court or individual Justices have . . . found at least the roots of that right in the First Amendment, . . . the Fourth and Fifth Amendments, . . . the penumbras of the Bill of Rights, . . . the Ninth Amendment, . . . [and] in the concept of liberty guaranteed by the first section of the Fourteenth Amendment.") (emphasis added).

of a fundamental right to data privacy, the data privacy laws in the United States are based largely in principles of tort and contract law, which can be conflicting.[40] This is in stark contrast to the EU, where the right to privacy is specifically guaranteed.[41]

2. Court Precedential Barriers

In addition, the First Amendment also causes problems for U.S. data privacy law reform. One company has successfully made the argument that prohibitions on the use of consumers' information violates businesses' right to freedom of speech.[42] Another instance where the Supreme Court has not advanced consumer data privacy interests was in *Sorrell v. IMS Health*, where the Court held that a pharmaceutical company should be allowed to access doctors' prescribing records or they would be denied the ability to better target potential new customers.[43] Furthermore, courts have also regularly found that data privacy violations are not a cognizable injury,[44] and an advertiser's use of private information does not deprive a consumer of monetary benefit.[45]

3. Federal Privacy Law Failures

Not only have the courts held up privacy law in this area, but several federal data privacy laws fail to help consumers because they are narrowly focused. The Fair Credit Reporting Act (FCRA) allows credit agencies to disclose personal information as long as they implement "reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer."[46] The Gramm–Leach–Bliley Act (GLBA) later added more to the FCRA, requiring financial institutions to notify customers of how their information is used and afford them the ability to opt out of disclosure to third parties, prohibiting the disclosure of account numbers to third parties, and requiring the FTC to create a Safeguards Rule for businesses.[47] The Cable Communications Policy Act (CCPA) requires cable companies to

40. *See* Hoang, *supra* note 12, at 818, 843 (explaining the complexity of having contract law, tort law, and federal and state statutes governing data privacy; for example, contract law would require a company to provide notice, choice, and access to share information; however, under tort law, if the company is deemed negligent, they are held to the same duty of care as other companies in the industry; in addition, federal and state laws may be involved as well).

41. *See generally* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (addressing the protection of individuals in regards to the processing of personal data).

42. *See* Sorrell v. IMS Health, Inc., 564 U.S. 552, 591 (2011) (finding that the First Amendment should also protect the "marketplace of ideas").

43. *See id.* at 562 (stating that the relevant statute "unconstitutionally burden[ed] the speech of pharmaceutical marketers and data miners without adequate justification").

44. Brookman, *supra* note 10, at 365 (citing as an example *In re* Google, Inc. Privacy Pol'y Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *13 (N.D. Cal. Dec. 3, 2013) failing to find a cognizable injury when defendant Google used plaintiff's likeness).

45. *Id.* (citing *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434 (D. Del. 2013); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1032 (N.D. Cal. 2012); *In re* Sci. Applications Int'l Corp. Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014)).

46. 15 U.S.C. § 1681(b) (2012).

47. Hoang, *supra* note 12, at 822.

disclose to customers how their private information is being used.[48] The Health Insurance Portability and Accountability Act (HIPAA) requires businesses possessing private health information to provide customers with notice of dissemination, a way to opt out, access to information at any time, and secure transmission of information.[49] The Computer Fraud and Abuse Act (CFAA) only applies to businesses who suffer a data security breach due to "the negligent design or manufacture of computer hardware, computer software, or firmware," and requires the plaintiffs to show they experienced more than $5,000 in damages.[50] Section Five of the FTC Act has only recently been applied to data privacy and is a catch-all for businesses not regulated by the other federal laws.[51]

4. Enforcement Problems

The problem with the U.S. model is partially due to how the privacy laws are enforced. The FTC is responsible for enforcing online privacy laws.[52] However, the FTC cannot independently act to stop wrongdoing unless the business is breaching its own privacy policy.[53] The FTC has applied the FTC Act to cases involving businesses' misuse of private information where the FTC can show that "a consumer was deceived, or where a business practice is objectively 'unfair' because it (1) causes significant consumer harm that (2) is not avoidable by consumers and (3) is not offset by countervailing benefits."[54] In addition, the FTC finds that poor data security practices meet this standard if "(1) they lead to exposure of sensitive personal information, (2) they are not detectable or auditable by consumers, and (3) the costs of implementing better policies is far less than the damage done by the poor security practices."[55] The FTC has recently endeavored to bring cases against businesses that made flagrant misrepresentations in their privacy policy[56] and also against businesses that omit surprising data policies to consumers (the FTC made allegations against Path, a social network that did not tell consumers clearly that it was accessing consumers' contact information on users' phones).[57]

Relatively recently, several states have begun to pass legislation requiring businesses to notify consumers when there has been a data breach, with 47 states currently implementing these laws.[58] However, this recent proliferation of state legislation can make it difficult for a business to know what their "level of responsibility" is when it comes to providing protection to consumers from different states and, in turn, which profitable practices are off limits.[59] Some states base their privacy laws on a contract theory, while

48. 47 U.S.C. § 551 (2001).

49. Hoang, *supra* note 12, at 822.

50. 18 U.S.C. §§ 1030(a)(4), (g) (2008).

51. 15 U.S.C. § 45 (2006); Hoang, *supra* note 12, at 822.

52. Hoang, *supra* note 12, at 826.

53. *Id.*

54. Brookman, *supra* note 10, at 358.

55. *Id.*

56. *Id.* (citing FTC v. Toysmart.com, LLC, No. Civ. A. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000)) (asserting FTC's claim that Toysmart shared consumer information despite asserting in its privacy policy it would not share information); In the matter of Eli Lilly & Co., 133 F.T.C. 763 (2002) (asserting the FTC's allegation that Eli Lilly & Co. shared consumer information despite its own privacy policy).

57. Brookman, *supra* note 10, at 358–59.

58. Peters, *supra* note 22, at 1181 ("Only Alabama, New Mexico, and South Dakota do not currently have notification laws.").

59. Hoang, *supra* note 12, at 843.

others use a tort theory, resulting in inconsistent standards for businesses, expectations for consumers, and ultimately court rulings.[60] However, some states, like California, have gone as far as providing privacy protection in their own state constitutions.[61] In addition, states disagree on what constitutes "personal information" falling under the umbrella of the state's protection.[62] States with data breach notification laws all agree that if data is leaked, businesses only have to report a breach to consumers when the data was not encrypted or when the encryption key for the data was compromised.[63]

5. Corporate Barriers to Reform

Several large businesses have recently come together to oppose steps toward stricter pro-consumer privacy laws in the United States.[64] In 2013, California attempted to pass the Right to Know Act.[65] Before the Act, Californians could find out about disclosure of their information to third parties but only about disclosures a business made for marketing purposes.[66] Under the Act, Californians could ask for all the ways their personal information was being shared with third parties.[67] Before the Act could be passed, corporations like Facebook came together to oppose it.[68] Pressured by these corporations, the California legislature did not pass the Right to Know Act.[69]

Another example of corporations coming together to oppose more expansive personal information protection is the Spokeo media attack.[70] Corporations like Facebook and Google came to the aid of data broker Spokeo when the company came under fire for inaccurate credit reports.[71] Spokeo claimed that its consumers had to prove that they

---

60. *Id.*

61. CAL. CONST. art. 1 § 1 (guaranteeing a fundamental right to privacy: "[a]ll people are by nature free and independent and have inalienable rights. Among these are . . . privacy").

62. *See, e.g.*, *Data Breach Charts*, BAKERHOSTETLER 2 (2014), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf (comparing, for example, Alaska and Arkansas: Alaska includes passwords, personal identification numbers, or other access codes to financial accounts; Arkansas does not include any of those elements, but does add medical information).

63. Peters, *supra* note 22, at 1182.

64. *See infra* note 65 (discussing large corporations gathering resources to oppose a California Act that would have increased protection for consumer information); *infra* note *73* (discussing large corporations encouraging the Supreme Court to rule in favor of a data broker).

65. *See* A.B-1291, 2013–2014 Reg. Sess. (Cal. 2013), http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1291 (introducing the Right to Know Act of 2013).

66. *See* Rainey Reitman, *New California "Right to Know" Act Would Let Consumers Find Out Who Has Their Personal Data—And Get a Copy of It*, ELEC. FRONTIER FOUND. (Apr. 2, 2013), https://www.eff.org/deeplinks/2013/04/new-california-right-know-act-would-let-consumers-find-out-who-has-their-personal (stating the proposed legislation "make[es] it possible for California consumers to request an accounting of all the ways their personal information is being trafficked—including with online advertisers, data brokers, and third-party apps").

67. *Id.*

68. *Id.*

69. Jeff Blagdon, *California's Right to Know Act stalls after opposition from tech lobby*, THE VERGE (May 6, 2013, 9:29 PM), http://www.theverge.com/2013/5/6/4306896/california-right-to-know-act-stalls-after-opposition-from-tech-lobby.

70. Brookman, *supra* note 10, at 366 n.69.

71. *Id.* at 366.

sustained a cognizable harm[72] and was aided by amicus briefs filed by corporations.[73] These large corporations had also faced many lawsuits over privacy rights violations where they believed there was no tangible harm.

B. The EU Model

The EU model differs from the U.S. model in several ways. To begin, the EU recognizes an explicit right to privacy for each citizen.[74] The European Convention on Human Rights states that Europeans have a "right to respect for . . . private and family life."[75] In addition, several constitutions of European nations protect the rights even further (Germans enjoy the right to informational self-determination and communication privacy, and the French also enjoy a right to have their private lives respected).[76]

Along those same lines, it is generally accepted throughout Europe that any information pertaining to an individual is defined as "personal."[77] The right to data privacy is also bolstered and enforced by Directive 95/46/EC, also known as Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Directive).[78]

The Directive requires businesses that collect data to inform consumers of: (1) why they are processing data; (2) the "obligatory or voluntary" nature of a reply to the request to process data; (3) consequences of failing to reply; (4) the "categories of recipients" of the data; and (5) the consumer's right to access and correct data.[79] The Directive also restricts collection of information relating to "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[80]

The EU created an independent supervisory agency to enforce the Directive that oversees data privacy throughout the EU.[81] This agency may intervene when a business does data processing in the EU and they are established there.[82] The agency also may intervene when the business is not in the EU but either national law applies because of public international law or where equipment is used in the EU to process data.[83] In addition, the Directive mandates that each member state provide its own independent agency to enforce data privacy laws.[84] The way each member state forms the agency is up to the

---

72. *Id.*

73. Brief for eBay Inc. et al. as Amici Curiae Supporting Petitioner, Spokeo, Inc. v. Robins, 135 S. Ct. 1892 (2015) (No. 13-1339), 2015 WL 4148654, 2015 WL 4148654, at *4 (Jul. 9, 2015) (asking that the Court must rule on this issue to resolve a circuit split and arguing that there was no cognizable harm in this case).

74. Directive 95/46/EC, *supra* note 41.

75. European Convention on Human Rights art. 8, June 1, 2010.

76. James, *supra* note 14, at 260.

77. *Id.*

78. Directive 95/46/EC, *supra* note 41.

79. *Id.* at art. 10

80. *Id.* at art. 8(1).

81. Council Regulation 45/2001, of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals With Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, ch.1, art. 1(2), 2000 O.J. (L 8) (creating and empowering the European Data-Protection Supervisor to enforce the Directive amongst the EU member states).

82. Directive 95/46/EC, *supra* note 41, at art. 3(1).

83. *Id.* at art. 4.

84. *Id.* at introductory cmt. 65.

state, with some nations including government officials and others utilizing independent individuals not affiliated with the government.[85] The Directive also provides that member states must have an accessible avenue for wronged consumers to pursue litigation and obtain remedies.[86] In addition, businesses in EU countries cannot share data with non-EU countries unless those countries have adequate data privacy laws in line with the Directive.[87]

However, state-by-state application of the Directive is not without flaws. In the United Kingdom (UK), an independent agency free of government involvement, the Informational Commissioner's Office (ICO), enforces the country's data privacy laws.[88] The ICO has been criticized as "toothless and inept," being especially unwilling to take on large media conglomerates and failing to bring businesses up to speed on the latest data privacy laws.[89] In France, the Commission on Information Technology and Liberties (CNIL) enforces data privacy laws, but unlike their counterpart in the UK, CNIL is integrated into the country's government.[90] CNIL does have some power in that businesses wishing to house private information must gain approval from the agency.[91] CNIL also does have considerable investigatory and monitoring power and the ability to impose hefty sanctions.[92] However, CNIL has come under fire for being too connected to the government and, among other things, protecting government interests rather than citizens' right to data privacy.[93] In addition, the EU still suffers from data breaches despite its reportedly strict data privacy regime.[94]

III. ANALYSIS: PROPOSED SOLUTIONS TO THE U.S. DATA PRIVACY PROBLEM

The United States has a data privacy problem.[95] Laws designed to protect consumers' private information are not up to date with the current technologies.[96] The lack of strong regulations makes it difficult for government agencies to enforce protections.[97] On top of it all, the United States relies on a system of self-regulation where businesses regulate themselves and face a clear conflict of interest between profit and protection.[98]

There are several proposed methods to strengthen U.S. data privacy law and enforcement.[99] Some have suggested the U.S. model can be saved.[100] Others suggest that

85. Hoang, *supra* note 12, at 817.
86. James, *supra* note 14, at 282.
87. Directive 95/46/EC, *supra* note 41, at introductory cmt. 56.
88. Hoang, *supra* note 12, at 832.
89. *Id.* at 836–37.
90. *Id.* at 838–39.
91. *Id.* at 840.
92. *Id.* at 839–40.
93. Hoang, *supra* note 12, at 840.
94. Philip N. Howard & Orsolya Gulyas, *Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005–2014*, (CEU Sch. Pub. Pol'y: Ctr. Media, Data, & Sec., Working Paper 2014), http://cmds.ceu.edu/article/2014-10-07/data-breaches-europe-reported-breaches-compromised-personal-records-europe-2005#sthash.9UYtQ9m3.dpuf.
95. *See supra* Part II.A (describing generally the privacy problem in the United States).
96. *Id.*
97. *See supra* Section II.A.1 (outlining criticisms of the U.S. model for regulating private consumer data).
98. *See supra* Part II.A (outlining the U.S. model for regulating private consumer data).
99. *See infra* Part III.A–C (analyzing proposed solutions to the U.S. data privacy proposal).
100. *See generally* Maxwell, *supra* note 35 (detailing data that shows consumers stick with default

adoption of portions of the EU model will make the best improvement.[101] In addition, proponents of other models have offered their opinions on how their approach would fare in the United States.[102]

A. Keeping the Current U.S. Model

1. Continued Self-Regulation

Some suggest the existing U.S. model can heal itself by continued self-regulation.[103] Supporters of self-regulation argue that businesses will continue to increase protections for a competitive edge within their market.[104] However, studies show that consumers could not care less about which company provides more data protection.[105] Facebook, Google, and other large companies have supported the self-regulation model, asserting that freedom to use private information assists valuable innovation without harming the consumer.[106] However, wronged consumers and their attorneys have argued that what these companies do with consumer information *does* harm consumers.[107] But even if a consumer wanted to take action against data collection, tracking the harm is often difficult because consumers usually have no idea how or when their data is being collected.[108] In the rare cases where consumers are aware their data has been collected, accessing businesses' opt-out mechanisms is difficult.[109] Critics of self-regulation also argue that it requires litigation as part of its regulatory framework, and such litigation can be difficult and expensive to carry out in the United States.[110]

2. Private Right of Action and Increased Litigation: Where is the Harm?

Supporters of bolstering the U.S. model suggest that it would perhaps help to give part

---

preferences and suggesting "opt-in" settings as a solution).

101. *See generally* Hoang, *supra* note 12 (comparing and contrasting EU and U.S. privacy law, and suggesting a reasonable middle ground for regulation).

102. *See generally* Dennis D. Hirsch, *Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons it Holds for U.S. Privacy Law*, 2013 MICH. ST. L. REV. 83 (2013) (describing the Dutch data privacy scheme, and making recommendations to adopt certain provisions of the Dutch privacy scheme).

103. Maxwell, *supra* note 35, at 62.

104. *See id.* at 62–63 (detailing the schools of thought concerning government involvement in online privacy practices).

105. *See id.* at 68 (citing studies showing that consumers are often unaware of what practices they are consenting to when they sign up for services, to the point where they cannot give meaningful consent); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 667 (2014) (citing empirical evidence that privacy policies are not being read or understood).

106. *See* Maxwell, *supra* note 35, at 64 ("[Facebook's] comment explains that Google used geographic knowledge in connection with certain searches to find flu trends, and Netflix used past rental orders to customize viewing recommendations for subscribers.").

107. *See In re* Google, Inc. Privacy Pol'y Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *5 (N.D. Cal. 2013) ("[I]njury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff's personal identification information. Rather, a plaintiff must allege how the defendant's use of the information deprived the plaintiff of the information's economic value. Put another way, a plaintiff must do more than point to the dollars in a defendant's pocket; he must sufficient[ly] allege that in the process he lost dollars of his own.").

108. Maxwell, *supra* note 35, at 66 (citing a study that found that 25% of consumers did not know they had any options when it came to choosing how a company used their personal information).

109. *See id.* at 64–65 (discussing principles related to data transparency and consumer behavior).

110. *See id.* at 67 (examining the shortfalls of self-regulation).

of the responsibility to the people to regulate industry through litigation.[111] Currently, citizens can sue for data breaches under a few narrowly-cabined statutes like HIPAA and GLBA.[112] However, when individuals decide to bring actions under a statute, those statutes are rooted in principles of contract law.[113] Suing under data privacy statutes that are based on contract law presents problems: the plaintiffs in these cases often claim the business breached their contract not to share their information only to find their claims are precluded because they have already signed away their privacy rights in a Terms of Use Agreement.[114]

Others argue that the United States needs to pass new federal privacy laws based on the FIPPs.[115] The FTC recently suggested that Congress pass new legislation for a data privacy standard based on these principles.[116] The legislation should also include a private right of action, giving citizens an easier path to sue offending businesses.[117]

A private right of action would assist with the difficulty plaintiffs have with showing concrete harms in these cases.[118] Specifically, a private right of action is helpful because consumers do not technically "own" their personal information and sometimes the information leak has not yet caused a tangible harm.[119] The private right of action would allow more plaintiffs to sue successfully without having to show damages (necessary under the tort and contract law foundations of current data privacy laws) and provide important precedent for future litigation.[120] Such legislation would have helped plaintiffs like those in *In re Facebook Litigation* where the FTC settled with Facebook after the company broke a promise to the plaintiffs and sold their information to third parties.[121] The plaintiffs ended up with no remedial damages.[122] Although Congress has attempted to make strides in the area of data privacy protection, its most recent attempt, the Consumer Privacy Bill of Rights Act, did not include a private right of action.[123]

Some have argued that the current self-regulatory approach can work if you make a legally cognizable harm out of breaching privacy policies "beyond that of mere misrepresentation[s]" by the business.[124] Misrepresentations are not a sufficient standard on which to sue companies because companies know better than to blatantly violate their privacy policies, instead wording agreements carefully and broadly, taking advantage of the many ways to misuse private information.[125] Also, these companies can constantly

111. Hoang, *supra* note 12, at 849–50.

112. *Id.* at 850.

113. *Id.*

114. *See id.* (discussing plaintiff's waiver of rights by contract).

115. Alec Wheatley, *Do-it-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation with a Private Right of Action*, 45 GOLDEN GATE U. L. REV. 265, 283 (2015); Brookman, *supra* note 10, at 359.

116. Wheatley, *supra* note 115, at 283.

117. *Id.*

118. *Id.*

119. Hoang, *supra* note 12, at 850.

120. Wheatley, *supra* note 115, at 283.

121. *See generally In re* Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011) (discussing the sale of plaintiff's information to third parties).

122. Wheatley, *supra* note 115, at 284.

123. CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015, at 21 (Discussion Draft 2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [hereinafter CONSUMER PRIVACY BILL OF RIGHTS].

124. Maxwell, *supra* note 35, at 72.

125. *Id.* at 73.

change their policies and are often much more sophisticated parties than the consumer.[126] Making a legally cognizable harm would require giving consumers more control over what parts of their information was shared with third parties.[127]

Overall, it seems that a private right of action would at least provide more support to a struggling system. However, for reasons explained already in this Note and presented later, it may not be enough.[128] For Congress to add these private rights of action, they first have to pass the legislation, which is unlikely given their track record.[129] Even if Congress passes legislation, it would still be difficult for a consumer to discover that a business has leaked or sold their information unless it was a very public leak or the sale was somehow made public. The FTC is an entity that could have the capability to expose businesses that violate data privacy standards and help consumers gain more control and bring more actions.[130]

3. The FTC is Catching Up

Supporters of the current U.S. model point to recent, more aggressive attempted changes by the FTC that could strengthen data privacy law enforcement.[131] The FTC has pushed Congress to increase data privacy protections.[132] Recently, the agency proposed that mobile operating system providers must send notice to consumers every time their data is about to be shared with a third party.[133] As mentioned earlier in this Note, the FTC has urged Congress to adopt sweeping federal data privacy laws.[134] In addition, they have tried to use their existing statutes, like Section Five of the FTC Act, in new ways—for example, labeling data security breaches as "unfair trade practice[s]."[135] However, because businesses are not put on notice of these new ways to interpret existing statutes, they fail to bind businesses.[136] In addition, it will be easier for the FTC to protect consumers if Congress passes these regulations into law.[137]

The FTC could, over time, strengthen its regulatory power by clearly defining its jurisprudence under Section Five of the FTC Act; for instance, by "clearly defining the role [of] a company's knowledge of deception or intent to deceive."[138] These moves could put companies on notice and provide a pattern that could lead to increased enforcement. The

126. *Id.*

127. *Id.* at 72–73.

128. *Infra* Part III.C.

129. *See id.* (discussing Congressional failure to pass pro-consumer data privacy bills in 2012).

130. *Infra* Section III.A.3.

131. Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA HIGH TECH. L.J. 483, 521–22 (2015).

132. *Id.*; *see* Wheatley, *supra* note 115, at 281–83 (describing the breadth of the FTC's aggressive agenda for more data privacy protections).

133. Bagley & Brown, *supra* note 131, at 521–22.

134. *See supra* Section III.A.2 ("The FTC recently suggested that Congress pass new legislation for a data privacy standard based on these principles. The legislation should also include a private right of action, giving citizens an easier path to sue offending businesses.").

135. Hoang, *supra* note 12, at 852.

136. *See id.* at 852–53 ("If agencies were focused on prevention and performing assessments, companies would have notice about what is expected of them and, hopefully, would be less susceptible to breaching data security laws.").

137. *Supra* Section II.A.1.

138. Solove & Hartzog, *supra* note 105, at 668.

FTC is working toward these clarifications by attempting to punish violations of consumer expectations and implied representations.[139] Some even assert that the FTC has recently begun to develop a set of clear, strict standards that are based on industry practices.[140] Those arguing that the FTC can be effective claim the agency can now go after more offending businesses as they increasingly find that consumer-friendly standards are implied terms in privacy policies, and that consumer expectations hold weight.[141]

On the whole, it seems that the FTC is gaining some traction in the area of enforcement.[142] However, without the legal framework in place, the FTC is limited as to what it can accomplish.[143] The FTC may be able to regulate businesses better if it works in tandem with the States.[144]

4. Leave it to the States

In some ways, states could be the answer to the U.S. data privacy problem, as some have made greater strides than Congress with regard to effective laws.[145] The FTC can enforce strict state laws if the state law prohibits deceptive practices, because Section Five of the FTC Act prohibits those same practices.[146] This would allow a state-federal government relationship not unlike the EU-member states' relationship, where states implement the recommendations and statutes of the larger entity. In addition, some have suggested that state regulatory agencies and the FTC could tag-team handling businesses' violations by passing legislation that allows the FTC to bring an enforcement action.[147]

States are also free to implement recommendations by the FTC that Congress is reluctant or slow to pass into law.[148] For example, California can pass strict regulations, like their statute requiring companies to make public commitments about information they are collecting from consumers.[149] Increasing state regulation and federal-state cooperation could help consumers stay protected.

This tandem approach may work, though it seems more complicated to have a federal agency enforce and assist with state laws. To make this relationship work, the FTC still has to convince states to adopt similar laws that it can help enforce. Ultimately, this solution is contingent on each individual state changing its laws.

---

139. *See id.* at 670 (citing a number of complaints the FTC has charged against companies that have violated privacy and security misrepresentations).

140. *See id.* at 672 (describing the FTC's regulatory regime due to an effort to detail requirements for companies to follow).

141. *See id.* at 673 (describing how the FTC's enforcement of detailed requirements can give more power to consumers).

142. *See supra* Section III.A.3 (discussing the strides the FTC has made in data privacy protection).

143. *See supra* Section II.A.1 (explaining how the self-regulated model the United States uses when enforcing its private information is ineffective against businesses).

144. *See infra* Section III.A.4 (describing how the FTC can enforce strict state laws efficiently rather than relying on Congress for effective regulation).

145. Gregory James Evans, *Regulating Data Practices: How State Laws can Shore up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 212 (2015).

146. *Id.* at 213; 15 U.S.C. § 45 (2006).

147. Evans, *supra* note 145, at 214–15.

148. *Id.* at 203.

149. *Id.* at 213.

B. Adopting the Enforcement Framework of the EU Model

Many are convinced that a wholesale adoption of the EU model would not work. There are several reasons for this, at the core of which is the fact that the EU model is built on an assumption of a universal right to privacy.[150] Conversely, the U.S. Constitution does not recognize an explicit strong right to data privacy.[151] In fact, U.S. citizens do not even technically "own" their personal information.[152]

However, one of the essential components the United States could borrow from the EU model would be an independent data protection agency to regulate industry.[153] The United States currently relies mainly on the FTC, but also on other agencies to regulate.[154] Consolidating would make the process more efficient and enable the agency to adapt more quickly to technological advances.[155] The independent agency should have the ability to institute fines to deter businesses from committing violations.[156] There is already precedent for agencies stepping in to regulate, whether it is the FCC regulating media or the government fining corporations for violating environmental law.[157]

In addition, the U.S. policy could use a shift in its entire focus to align more with what the EU is doing. Currently, the FTC and the Department of Commerce only act on breaches that have already occurred.[158] In the EU, data protection agencies not only respond to breaches, but are more actively involved in intervening to prevent consumer data breaches.[159]

However, there may be trouble in the EU, as it has recently been reported that many member states are seeking to soften the EU Directive.[160] Little is known about the reasoning behind reform, but one could assume that the EU would like to free up its economy to make it more like that of the United States. Recently, Europe's highest court struck down a deal between the United States and the EU whereby private information could be transferred between the countries.[161] This type of ruling could create tension, as the EU could probably benefit from working with large American tech companies like Apple and Google. Member states have also expressed varying views on what data protection should look like.[162] Perhaps the same result could occur if sweeping federal laws were passed in the United States and the states had differing opinions.

To adopt a model more like the EU's, the United States would still have to pass new legislation. At the very least, it seems that there are some issues with the EU's data privacy regime, whether it is trying to help the economy by freeing up information or keeping the

---

150. *See supra* Part II.B (discussing foundations of the EU model).

151. *See generally* U.S. CONST. (note that it does not explicitly mention privacy).

152. Hoang, *supra* note 12, at 850.

153. *Id.* at 817.

154. *Id.* at 850–51.

155. *See id.* at 851 (stating that non-consolidation leads to inefficiencies).

156. *Id.* at 851–52.

157. Hoang, *supra* note 12, at 851–52.

158. *Id.* at 852.

159. *Id.*

160. Nicole Sagener, *Member states hope to soften data protection in reform talks*, EURACTIV (Mar. 5, 2015, 1:16 AM), http://www.euractiv.com/sections/innovation-industry/member-states-hope-soften-data-protection-reform-talks-312639 (last updated Oct. 15, 2015, 5:29 AM).

161. Mark Scott, *Data Transfer Pact Between U.S. and Europe Is Ruled Invalid*, N.Y. TIMES (Oct. 6, 2015), http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=1.

162. *Id.*

system unified.

C. Collaborative Governance Approach

An interesting new development in the discussion about how to fix the U.S. data privacy regime is that of "collaborative governance," an approach the United States seems to be considering.[163] As the name implies, collaborative governance involves the government working together with businesses to create a regulatory framework that both protects consumers and the businesses themselves.[164] Under this approach, the government drafts a broadly-worded statute that requires businesses to handle consumer data in certain ways.[165] Then, businesses take this broad statute and draft "codes of conduct" that apply the statute to their particular industry and the situations they encounter.[166] The FTC approves each code and businesses that do not violate the codes have "safe harbor."[167] Likewise, if businesses violate the codes they helped draft, they are subject to governmental regulation.[168]

There are several pros and cons associated with this approach. Unlike current U.S. regulation, which is by its nature adversarial (pitting public interest groups, industry giants, and the government against each other), the collaborative approach gives hope to the idea that businesses can reach workable solutions and also protect consumers.[169] Still, there is the possibility that businesses could manipulate the codes of conduct and the government may not be able to keep up in its enforcement.[170] Although many consider collaborative governance to be a middle ground between self-regulation and direct government interference, whenever an industry is allowed to regulate its own profit-gaining activities, there is going to be an obvious risk of abuse.

Some claim the collaborative governance approach helps enforcement and compliance because, rather than being regulated from the outside, businesses are more likely to feel a level of ownership and adhere to the codes they helped draft.[171] This assertion, however, is based on the idea that businesses will act like individuals, and the counterpoint still remains that businesses may abuse their power to create the codes. Critics also add that the more cooperative the governmental regulator gets with the industry, the more difficult it will be for the government to establish and enforce strict regulations.[172]

Proponents of this approach have some real-world results to back up their claims, as the Dutch have adopted the collaborative governance model to regulate how businesses use consumer data.[173] The Dutch draft broad statutory requirements, then the industry drafts codes which a governmental regulator approves, and if firms do not violate the codes then they enjoy safe harbor.[174] The most puzzling component of the Dutch system is that

163. Hirsch, *supra* note 102, at 86–87.
164. *Id.* at 87–88.
165. *Id.* at 86–87.
166. *Id.* at 87.
167. *Id.*
168. Hirsch, *supra* note 102, at 97.
169. *Id.* at 88.
170. *Id.*
171. *Id.* at 104.
172. *Id.* at 107.
173. Hirsch, *supra* note 102, at 123.
174. *Id.* at 89.

businesses agree to do it.[175] At the beginning of the system's implementation and the rolling out of broad statutory regulations, businesses were confused as to how to apply them or what constituted a violation.[176] This could be compared to the situation encountered by businesses in the United States that are subject to a wide array of differing state data privacy laws.[177] However, the Dutch industry saw the broad statutes and opportunity to draft codes as a chance to achieve regulatory certainty.[178] In addition, creating codes of conduct meant stopping future direct government regulation that could end up being more stringent.[179] The industry's acceptance sent positive signals to the public and to the legislature.[180]

The Dutch policy is not without issues. Critics see the system as "slow-moving and static, not nimble and adaptive."[181] Studies have found wide-spread noncompliance and a lack of resources to enforce violations.[182]

The United States actually appears to be considering this approach.[183] The collaborative governance model was basically set forth in three bills and the White Paper—a letter from the President which, among other things, advocates for "development of 'appropriate, legally enforceable codes of conduct' through the cooperation of private and public stakeholders," a "Consumer Privacy Bill of Rights," with the FTC enforcing those rights, and requiring businesses' recognition and cooperation.[184] The bills and White Paper are different than the Dutch program in several ways, in some cases an improvement and in some cases a step backward. Unlike the Dutch policy, the proposed U.S. policy does not restrict codes to certain industry sectors; it also allows public interest groups and others to weigh in on codes.[185] To its detriment, the U.S. policy is not comprehensive in that it does not extend safe harbor to all statutory requirements.[186] In addition, the U.S. policy's biggest flaw, by no fault of its own, is that there currently is not a broad data protection statute for businesses to interpret.[187] The White Paper calls for congressional action in this regard.[188]

Regrettably, the bills failed to pass in 2012. Earlier in 2015, a new iteration of the bill was proposed, entitled the Consumer Data Privacy Bill of Rights Act.[189] The Act establishes certain requirements for the codes of conduct drafted by businesses, including

---

175. *Id.* at 125–26.

176. *Id.* at 125.

177. *See supra* Section II.A.4 (discussing the varying state laws and how businesses struggle to know which standard they must meet).

178. Hirsch, *supra* note 102, at 126.

179. *Id.*

180. *Id.*

181. *Id.* at 151.

182. *Id.* at 151–52.

183. Hirsch, *supra* note 102, at 86–87.

184. *Privacy, Data Security, and Information Law Update: White House Issues First Ever Administration-Level Data Privacy Framework*, SIDLEY AUSTIN LLP 1 (Feb. 29, 2012), http://www.sidley.com/~/media/Files/News/2012/02/White%20House%20Issues%20First%20Ever%20AdministrationLeve__/Files/View%20Update%20in%20PDF%20Format/FileAttachment/2272012%20Privacy%20update; CONSUMER PRIVACY BILL OF RIGHTS, *supra* note 123.

185. Hirsch, *supra* note 102, at 120–21.

186. *Id.* at 122.

187. *Id.* at 121.

188. *Id.*

189. CONSUMER PRIVACY BILL OF RIGHTS, *supra* note 123.

requiring businesses to "provid[e] consumers with clear notices about how their personal details will be collected, used and shared."[190] The bill is still being discussed in Congress, but many are doubtful that it will pass.[191]

Even if the Act did pass, it would be difficult to get U.S. businesses to buy into a collaborative governance scheme that would require them to divulge critical information to regulators, which may include public interest stakeholders.[192] However, the system could be ideal, as the United States has many more resources at its disposal than the Dutch.[193] In addition, the many years of an adversarial style could help with negotiating codes of conduct more effectively.[194] The United States's greater amount of resources may also solve the problem the Dutch have with noncompliance and slow-moving adaptation.

IV. RECOMMENDATION

The United States should adopt a new regime incorporating several concepts from the various models suggested by scholars, the government, and other countries. Although each approach has its strengths, it will take a weaving together of many different proposals and foreign legislative examples to fully protect consumers' personal information. A simple application of the EU model will not work because there is no explicit right to privacy on which to build.[195] Creating an independent agency to enforce governmental regulations could cause more conflicts and may not be powerful enough.[196] Including a private right of action in privacy law could help consumers, but it is ineffective when consumers are ill-informed of when their data is leaked or sold. Therefore, an inclusive approach is warranted.

The first step to protecting consumer data would be to begin to recognize a fundamental right to privacy of certain personal information. The United States should adopt a portion of the EU model, which extends the fundamental right to privacy to personal information contained in consumers' data. This consumer data would include every bit of information about the consumer, from location to medical records. When privacy of personal data is recognized as a fundamental right, that information can no longer constitutionally be bought and sold on the open market as property.

The United States should next create a new regulatory framework to protect against consumers signing away their rights to their information and also their ability to find out what becomes of their information. Congress should revisit passed Acts that were opposed by pro-business opposition, like the Consumer Privacy Bill of Rights Act.[197] The federal

190. Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. TIMES (Feb. 27, 2015), http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?_r=2.

191. *See id.* (discussing how many doubt the bill will pass even though it is still being discussed by Congress).

192. *See* Hirsch, *supra* note 102, at 154 (discussing how it would be difficult to convince U.S. businesses to buy into collaborative governance scheme that would require the businesses to divulge critical information).

193. *Id.* at 162.

194. *Id.*

195. *See* Directive 95/46/EC, *supra* note 41 (providing a right to privacy); Hoang, *supra* note 12, at 853 (distinguishing the United States from EU law in this regard).

196. *See supra* Part II.B (relating the experience of the UK implementing an independent agency that is seen as toothless and unwilling to go after large corporations).

197. CONSUMER PRIVACY BILL OF RIGHTS, *supra* note 123.

government can also look for guidance from several states that have had success in implementing privacy regimes.[198]

Like the EU, Congress should return to the basic principles of the FIPPs to craft laws that will cover consumers. After all, there are many countries that require businesses to disclose to consumers what they are doing with private information and still have a stable economy.[199]

Congress should include in new federal data privacy laws a private right of action for consumers that have been wronged. Consumers should be able to sue based on their reasonable expectations of privacy because usually these businesses are much more sophisticated and currently take advantage of unwary consumers. Increased effective consumer-led litigation could provide a valuable incentive for businesses to adhere to new privacy laws that Congress would implement. Along those same lines, consumers should be better notified of what is being done with their information. Consumers are often asked to send random reports to companies when their apps crash or their program has a bug—the companies could send randomly generated reports of their information sharing activities. Alternatively, companies could simply post to the consumers' profiles or homepages what information they have shared and with whom.

New data privacy laws should also give more power to the FTC to regulate businesses and the ways they handle consumers' personal information. Currently, the FTC's power is too limited in that the U.S. model breaks up enforcement of laws into different industry sectors.[200] The FTC, if given the ability, could probably regulate consumer data effectively if given legislative support and help from the States.[201] Using an agency that is independent of the government could also be effective, but there have been mixed results in other nations.[202] There are current Acts that could be defined more concretely to let businesses know what they are required to disclose and what they are prohibited to do concerning consumer data.

Collaborative governance could play a key role in this new regime. Allowing businesses to sit in on the creation of these new laws could provide the leverage necessary to appease certain parties in Congress that are worried about harming the U.S. economy. The approach could be even more effective in the United States because of the resources available.[203]

V. CONCLUSION

In conclusion, the United States should create a new model for data privacy based on

198. *See* Evans, *supra* note 145, at 213 (discussing California's legislation requiring public commitment of private information businesses possess). However, keep in mind this same state failed to pass the Right to Know Act, an arguably more powerful piece of legislation.

199. *See supra* Part II.B (detailing how the EU functions on a system of heightened data security and disclosure—and even holds nations it does business with to that standard—and still keeps their economies afloat).

200. *See supra* Section II.A.1 (detailing criticisms of the U.S. self-regulating model).

201. *See supra* Section III.A.3–4 (detailing changes by the FTC that could strengthen data privacy law enforcement, and why states should be left with the power to answer U.S. data privacy problems).

202. *See supra* Part II.B (stating that the UK has implemented an independent agency that has been criticized as being too weak, while France uses an agency staffed by government officials that has been accused of being more concerned with protecting government interests rather than the privacy interests of the citizens).

203. *See* Hirsch, *supra* note 102, at 162 (positing that, with the United States's size, large government, adversarial culture, and consumer and privacy advocacy groups, the collaborative approach could be a success).

a combination of several approaches to protect consumers' private information. The elements of the EU Model that the United States could adopt would fare even better in the United States because of the vast amount of resources at the country's disposal. It would also make working with the EU easier, as they are concerned about the rising number of data breaches occurring in the United States.