Vanderbilt Journal of Entertainment & Technology Law

Volume 18
Issue 1 *Issue 1 - Fall 2015*

Article 5

2015

Secondary Data: A Primary Concern

Kelsey L. Zottnick

Secondary Data: A Primary Concern

ABSTRACT

This Note addresses privacy concerns implicated by rising secondary data mining. Secondary data mining is the use of personal information for a purpose other than the original. This complex technology drives billions of dollars in commercial industry yet remains largely unregulated. This Note examines the current state of the data mining industry and the behavioral fallacies that belie societal concerns about online privacy. Further, relevant federal, state, and constitutional laws appear outstripped by these technological advances. An analysis of potential privacy solutions examines the advantages and disadvantages of implementing each one through the privacy community, the federal government, and the private sector. Finally, this Note concludes that implementing a solution through any one entity would not sufficiently protect against privacy harms. As such, this Note proposes a coregulatory solution to treat secondary data's privacy concerns as a market failure. This solution offers a practical way to safeguard personal data while aligning incentives between third parties and users.

TABLE OF CONTENTS

"YOU are the product." So said Don Draper, famous fictional ad man from the television series *Mad Men*.[1] Decades later his words remain prescient. Americans are bombarded by advertising.[2] And that does not begin to describe the layer of advertising just beneath the surface of people's lives. This "subsurface" advertising is called the secondary data industry.[3] Secondary data is personal information used for purposes other than those originally given.[4] Often companies do not tell people they are using their information in alternate ways.[5] They collect, analyze, and experiment with secondary data to better target potential purchasers.[6] And this is only the beginning: secondary data threatens to know people better than they know themselves. The Target Company found this out firsthand by using

1. *See Mad Men: For Those Who Think Young* (AMC television broadcast Jul. 27, 2008).

2. *See* Louise Story, *Anywhere the Eye Can See, It's Likely to See An Ad*, N.Y. TIMES, (Jan. 15, 2007), http://www.nytimes.com/2007/01/15/business/media/15everywhere.html [http://perma.cc/QA9F-8U2L] (citing research that says Americans typically saw up to five thousand messages a day, up from two thousand a day thirty years ago).

3. *See, e.g.*, Tal Z. Zarsky, *'Mine Your Own Business!': Making the Case For the Implications of the Data Mining of Personal Information in the Forum of Public Policy*, 5 YALE J. L. & TECH. 1, 16–18 (2003) (describing how companies use secondary data to tailor advertising to potential consumers).

4. *See id.* at 33; *see also* "secondary data," CAMBRIDGE DICTIONARIES ONLINE, http://dictionary.cambridge.org/us/dictionary/english/secondary-data?a=business-english [http://perma.cc/CKR8-VNED].

5. *See* Zarsky, *supra* note 3, at 32.

6. *See id.* at 2–4.

secondary data to target shoppers' habits.[7] One consumer, upset that Target sent his high school daughter baby coupons using its secondary data tools, complained that such faulty analytics encouraged rather than predicted behavior.[8] When the manager called to apologize, the man backtracked, admitting he had not been aware his daughter was pregnant.[9]

Though Target's marketing methods may seem extreme, such secondary data use is becoming the norm. However, secondary data's rapid growth and eerie accuracy belie the host of privacy concerns that plague the unchecked use of other people's personal information.[10] For instance, the online dating site OkCupid responded to criticisms of allegedly manipulative behavioral testing by labeling privacy concerns passé.[11] OkCupid cofounder Christian Rudder famously stated, "OkCupid doesn't really know what it's doing. . . . But guess what, everybody: if you use the Internet, you're the subject of hundreds of experiments at any given time, on every site. That's how websites work."[12]

Dismissing privacy concerns does not make them disappear. Instead, these experiments expose third parties' current leeway to use personal online data as behavioral lab fodder.[13]

This Note addresses the current state of secondary data mining and offers a framework to reconcile the concerns of various stakeholders within a coregulatory model. Part I provides background on data mining and accompanying privacy concerns. It discusses the current state of relevant privacy laws in the federal, state, and constitutional spheres. Part II analyzes potential solutions to secondary data's privacy issues based on where the onus, or duty, to implement the solution lies. Part III proposes a coregulatory solution to secondary data use that seeks to harness the combined power of the

---

7. *See* Charles Duhig, *How Companies Learn Your Secrets*, N.Y. TIMES MAG., (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [http://perma.cc/C5FQ-MVG3].

8. *Id.*

9. *Id.*

10. Brian Fung, *OkCupid Reveals It's Been Lying to Some of Its Users*, THE SWITCH BLOG, (July 28, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/07/28/okcupid-reveals-its-been-lying-to-some-of-its-users-just-to-see-whatll-happen/ [http://perma.cc/SL33-EY75].

11. *See id.*

12. *Id.*

13. *See* Andrew Chin & Anne Klinefelter, *Content: Social Networks and the Law: Differential Privacy as a Response to the Reidentification Threat: The Facebook Advertiser Case Study*, 90 N.C.L. REV. 1417, 1420 (2012) (describing "databases of ruin" as a database's aggregation of private facts that could cause someone legally cognizable harm if released).

federal government and private sector in implementing a user-centric framework.

I. BACKGROUND

A. Data Mining

Data mining is the process of identifying behavioral patterns within data using algorithms.[14] It is broadly called a "sense-making application" because it culls volumes of raw information to extract useful knowledge.[15] Data mining not only uncovers existing behavior patterns, but forecasts future ones.[16] Indeed, it originated as a prognostic tool.[17] In the 1990s, GM researchers developed data mining to search databases for product defects that were not immediately obvious.[18]

The prerequisite to data mining is, of course, having data to mine. Lax legal parameters on data collection practices, discussed later in this Note, have propelled the secondary data industry's spread.[19] Currently, US businesses can track, aggregate, and sell private users' details to third parties as marketing profiles.[20] Popular companies like Facebook and Amazon maintain a robust trade selling user internet profiles to third parties.[21] Their privacy policies appear to mollify concerns by acknowledging data-collecting practices and requiring consent to use their sites.[22] However, these exchanges belie the extent to which third parties exploit user data for purposes unrelated to the original transaction.[23]

Data mining involves multiple steps. First, the company collects data from several sources.[24] Then the company decides what

---

14. *See* Zarsky, *supra* note 3, at 4; *see also* Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifiable Information*, 10 VAND. J. ENT. & TECH. L. 553, 555 (2008).

15. K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, para. 23 (2004).

16. Zarsky, *supra* note 3, at 4.

17. *Id.* at 7.

18. *Id.*

19. *See* Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Infinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 437 (2014).

20. *See id.*

21. *See id.* at 436 n. 8, 437, 448 (explaining that such companies indefinitely retain user data like buying habits, files, and posts to sell to third parties for marketing analysis).

22. *See id.* at 452–53.

23. *See id.* at 474.

24. *See Zarsky supra* note 3, at 8–9 (noting an insurance company used such data-mining sources as clients' payment information, other departments' policyholder histories, and clients' personal information from data brokers selling it in bulk).

data to mine.[25] The company culls potentially relevant information, a process called "data warehousing."[26] Data warehousing aggregates disparate bits of customer information with personal data purchased from third parties.[27] Then the data warehouse is stripped of unreliable or redundant data.[28] The remaining information is used for data mining.[29] Algorithms organize the remaining data and probe it to discover descriptive or predictive patterns.[30] Descriptive patterns reveal links between variables that allow researchers to pinpoint distinct categories of the dataset.[31] Researchers use these links to determine whether rules govern the associations.[32] Predictive patterns, meanwhile, allow researchers to derive future behaviors.[33] They can test data for potential behavior based on available data clusters or track long-term patterns.[34]

Data mining's complex and potentially invasive nature has earned it comparisons to the oppressive and nightmarish qualities of writer Frank Kafka's fictional world.[35] Data miners accumulate mounds of personal data so detailed and accurate that many people believe data miners "probably know more about you than your friends."[36] At the same time, data mining is reductive: it lumps users into rough profiles to sell to third parties.[37] Such processes enable companies to potentially discriminate against customers based on the data miners' stereotypes.[38] Finally, data mining may violate basic contract principles underlying users' interactions with websites.[39] Websites argue that users agree to be subjected to data mining

---

25. *Id.* at 8.
26. *Id.*
27. *Id.*
28. Taipale, *supra* note 15, at para. 40.
29. *See* Zarsky *supra* note 3, at 8.
30. *See id.*
31. *See id.* at 11.
32. *Id.* at 12.
33. *Id.* at 11.
34. *Id.*
35. Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 62 (2005); "Kafkaesque," OXFORD ENGLISH DICTIONARY, http://www.oxforddictionaries.com/us/definition/american_english/Kafkaesque [http://perma.cc/JYR2-ACRP].
36. Michael J. Milazzo, Note, *Facebook, Privacy, and Reasonable Notice: The Public Policy Problems with Facebook's Current Sign-Up Process and How to Remedy the Legal Issues*, 23 CORNELL J. L. & PUB. POL'Y 661, 681 (2014).
37. *See* Zarsky, *supra* note 3, at 22.
38. *Id.* at 25.
39. *See* Milazzo, *supra* note 36, at 668–69.

practices by consenting to use their sites.[40] But user consent to data mining practices remains largely illusory.[41] Most privacy policies do not clarify the essential terms of the deal.[42] Users often do not know how, when, or in what ways the website may use their personal data.[43] Nor are most users aware of the deal's financial imbalance. Users essentially pay for "free" social media websites with their personal information—to the tune of billions of dollars.[44] Such lack of effective notice arguably voids the idea that data mining is "consensual."[45]

B. Current Privacy Laws

A quick survey of current privacy laws in the United States reveals a clutter of largely outdated legislation. Federal laws are either stuck in the decades-old context in which they originated or only cover niche industrial sectors. Though some states have passed progressive privacy legislation, the myriad of evolving laws poses significant compliance problems. However, this legal landscape may offer valuable insights for building a more viable privacy legislation framework.

1. Federal Laws

a. Current Privacy Statutes

Current federal statutes provide scant privacy protection in this situation.[46] The 1986 Electronic Communications Privacy Act (EPCA) comprises Congress's attempt to offer broad protections for electronic communications.[47] Not much has changed since.[48] The

---

40. *See id.*; Brian Womack, *Facebook Experiment Draws Complaint from Privacy Group*, BLOOMBERG BUSINESSWEEK.COM, (July 4, 2014), http://www.bloomberg.com/news/articles/2014-07-03/facebook-experiment-draws-complaint-from-privacy-group [http://perma.cc/Y723-S8KP].

41. *See* Milazzo, *supra* note 36, at 685.

42. *See* Michelle N. Meyer, *Everything You Need to Know About Facebook's Controversial Experiment*, WIRED.COM, (June 30, 2014), http://www.wired.com/2014/06/everything-you-need-to-know-about-facebooks-manipulative-experiment/ [http://perma.cc/5NRE-XKG7]; *see also* Milazzo, *supra* note 36, at 685.

43. Milazzo, *supra* note 36, at 682.

44. *See id.* at 678.

45. *Cf. id.* at 675, 678 (arguing Facebook's "free" sign-up process encroaches on privacy because users do not expressly agree to terms underlying the exchange, namely Facebook's collection of user data).

46. Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 297 (2011).

47. *See* Electronic Communications Privacy Act of 1986 (EPCA), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2711, 3117, 3121–3127 (2013)).

EPCA contains several parts potentially applicable to consumer privacy issues.[49] However, closer inspection reveals that none provide meaningful safeguards for information in today's surveillance state.[50] For instance, the Federal Wiretap Act prohibits the federal government from intercepting electronic communications without a warrant.[51] The Act is relevant to privacy concerns because law enforcement uses data requests to force companies like Facebook to release user information.[52] Therefore, this Act seems to potentially shield people from so-called "fishing expeditions" into their private lives. However, it only prevents contemporaneous interceptions, which is little use for the vast majority of social media users' stored data.[53] Its reach is further limited by its application to solely governmental entities. In the same vein, the Stored Communications Act (SCA) is less expansive than its name suggests.[54] For example, communications stored for more than 180 days require only a court subpoena to be obtained.[55] But even those stored communications may not receive protection, because the SCA confines coverage to computer-network concepts based in the year 1986.[56]

b. Limited Privacy Protections of HIPAA and Other Industry-Specific Federal Laws

Other federal statutes may offer consumer privacy protections, albeit for ancillary reasons and to a more limited extent. For instance, the Health Insurance Portability and Accountability Act (HIPAA) protects patient information in the healthcare context.[57] The law

48. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213 (2004).

49. Lindsay S. Feuer, *Who's Poking Around Your Facebook Profile? The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy On Social Networking Sites*, 40 HOFSTRA L. REV. 473, 475 (2011).

50. Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third-Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 32–35 (2013).

51. 18 U.S.C. §§ 2510–2522.

52. *See* Josh Constine, *Spying and Police Requests for Facebook Data Up 24% Since 2014*, TECHCRUNCH, http://techcrunch.com/2014/11/04/facebook-government-requests/ [http://perma.cc/B6GQ-P733].

53. Bedi, *supra* note 50, at 32.

54. *See id.* at 33.

55. 18 U.S.C. §§ 2701–2711.

56. Kerr, *supra* note 48, at 1212–13; *see* Feuer, *supra* note 49, at 496 ("[T]he SCA 'does not easily apply' to social networking websites, as these websites do not fit within any of the categories enumerated in the statute.").

57. Womack, *supra* note 40; *see* Martha Tucker Ayres, Comment, *Confidentiality and Disclosure of Health Information in Arkansas*, 64 ARK. L. REV. 969, 977 (2011).

narrowly tailors how covered entities may use such information.[58] The law then limits "covered entities" to health plans, healthcare clearinghouses, or certain healthcare providers.[59] Further, the law provides consumers a right to receive notice about healthcare providers' disclosures to third parties, including breaches.[60] While HIPAA's contours appear to offer stout informational privacy, it has limited reach.[61] As previously stated, only covered entities must abide by HIPAA.[62] Therefore, data brokers are free to exploit medical information revealed outside HIPAA's bounds.[63] Data brokers sell lists of people's names, along with their accompanying medical conditions, to third parties, such as drug companies.[64] The companies shell out fees for access to these lists to learn which households suffer from such conditions as depression, erectile dysfunction, and Parkinson's disease.[65] Thus, if a data broker sells Jane Doe's information to her insurance provider, there is a possibility the provider could misconstrue Jane's healthcare data by incorrectly assuming certain things about her health based on her medications. But if the provider nonetheless relies on those incorrect assumptions to deny her coverage, there is nothing she can do about it.[66]

Other federal agencies have offered data privacy plans, from the White House's "Consumer Bill of Rights" to the US Department of Commerce's "Safe Harbor Framework" for personal data.[67] As with the Federal Trade Commission (FTC)'s standards, discussed below, compliance remains voluntary.[68] Similarly, though the Federal Drug Administration (FDA) regulates fitness devices that may accumulate medical data, its focus is on safety, not on privacy.[69]

---

58. *See id.* at 976–77.

59. *See Covered Entities*, HIPAA PRIVACY RULES, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/ [http://perma.cc/N3FJ-57P7].

60. *See* Ayres, *supra* note 57, at 985.

61. *See id.* at 972–73.

62. *See id.*

63. Womack, *supra* note 40, at 39.

64. *See* Ayres, *supra* note 57, at 972–73.

65. *Id.*

66. *See id.* (citing a case where an insurance company used inaccurate data purchased from a data broker to deny an otherwise healthy claimant life insurance).

67. *Consumer Bill of Rights*, WHITEHOUSE.GOV, (Feb. 23, 2012), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [http://perma.cc/6G54-9BQ9]; *Safe Harbor Frameworks*, EXPORT.GOV, http://www.export.gov/safeharbor/ [http://perma.cc/BT9K-CZHK].

68. *See id.*

69. *See* NY Times Editorial Board, *Smartwatches and Weak Privacy Rules*, N.Y. TIMES, (Sept. 15 2014), http://www.nytimes.com/2014/09/16/opinion/smartwatches-and-weak-privacy-rules.html [http://perma.cc/TC42-D9UQ].

c. The Federal Trade Commission's Involvement in Consumer Privacy

The FTC's Unfair or Deceptive Trade Practices Act arguably offers the strongest consumer privacy protections at the federal level.[70] The Act confers broad power on the FTC to act against companies who engage in "deceptive and unfair trading practices."[71] A practice may be "unfair" or "deceptive" when it likely causes substantial injury to consumers, consumers cannot reasonably avoid it, and its costs outweigh competitive or consumer benefits.[72] The FTC may challenge a commercial practice through administrative adjudication.[73] The FTC can issue regulations, specific orders, or civil penalties to enforce decisions against liable companies. Indeed, the FTC has accused various Internet services, including Facebook, of unfair trade violations with respect to consumer privacy.[74]

However, critics argue that the FTC's enforcement fails to address consumers' most salient privacy concerns.[75] A veritable taxonomy of potential privacy violations exists.[76] Many of these concerns, such as confidentiality breaches and information insecurity, result from inadequate privacy safeguards.[77] Critics contend that the FTC has failed to invoke preventative measures designed to prevent such violations from happening in the first place.[78] For example, one suggested set of preventative measures is called the "notice and choice" model.[79] This model has been trumpeted as a system allowing consumers control over their information.[80] As its name suggests, this model offers consumers upfront information about how the relevant site uses consumers' personal data, with the option to proceed or leave based on this information.[81] Though information asymmetry may

---

70. 15 U.S.C. § 45 (a); *see Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices*, CONSUMER COMPLIANCE HANDBOOK, (June 2008), http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf [http://perma.cc/AJ6X-9T9Y].

71. *See id.*

72. *See id.*

73. *See id.*

74. *See id.*

75. *See* Elspeth A. Brotherton, Comment, *Big Brother gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 569 (2012).

76. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

77. *See id.* at 490–91.

78. *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 327 (2013).

79. *See id.*

80. *See id.*

81. *See* Brotherton, *supra* note 75, at 577–78. ("[I]f the [Supreme] Court decides that people in general have notice of a risk, the Court treats any given individual as having consented to the risk as though the individual had both actual knowledge of the risk and an opportunity to reject it.").

render such "choice" illusory, the model nonetheless provides a starting point for data protection.[82] For example, in HIPAA, the notice and choice model requires specifics, such as identification of the possible third-party users.[83] But instead of requiring liable companies to adopt this baseline measure, the FTC usually defers to industry standards: it prosecutes companies for failing to comply with their own internal privacy policies.[84] By meeting companies on their own terms rather than holding them to higher standards, the FTC confines the results to self-regulatory pitfalls.[85] Critics suggest the FTC's neglect of front-end enforcement measures has contributed to the lack of meaningful privacy safeguards in the industry, despite the FTC's continued pursuit of violators.[86]

Further, the FTC faces several challenges in its quest to regulate secondary data practices.[87] First, its efficacy depends on forces outside its control.[88] Various factors, from public attitudes to political climate, shape the FTC's agenda and makeup.[89] Second, the FTC's limited enforcement abilities narrow its impact.[90] It pursues individual companies on the basis of individual incidents–responses that do not compel widespread consumer privacy reform.[91] Also, though the FTC's successful prosecution efforts may deter some consumer privacy violations, arguably the incremental nature of this process does not track emerging concerns.[92] Further, the FTC's expansive objectives require it to patrol a litany of consumer issues.[93] In sum, its limited resources and external pressures prevent it from meaningfully shaping consumer privacy protection.[94]

---

82. *See id.* at 587.

83. *See* Asay, *supra* note 78, at 326.

84. *See id.*

85. *See* Brotherton, *supra* note 75, at 569.

86. *See id.*

87. *See generally* Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED, http://www.wired.com/2012/06/ftc-fail/ [http://perma.cc/TC5J-74AU] (criticizing the FTC's efforts to protect consumer data privacy).

88. *See id.*

89. *See id.*

90. *See id.*

91. *See id.*; *see also* Stephanie A. Kuhlmann, *Legislative Update: DO NOT TRACK ME ONLINE: The Logistical Struggles Over the Right to Be Let Alone*, 22 DEPAUL J. ART TECH & INTELL. PROP. L. 229, 234, 250 (2011).

92. *See id.* (comparing the FTC to "a runner with two sprained ankles" due to its limited legal power and small staff).

93. *Id.*

94. *See id.*; FED. TRADE COMM'N, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [http://perma.cc/9B4B-BC8G].

2. State Laws

Many states have created their own consumer privacy rules to address the lacking federal response.[95] The result is a patchwork of evolving privacy laws.[96] On one hand, the laws offer safeguards for personal data in a variety of salient areas, from student-data privacy to email searches.[97] These laws enable states to address their citizens' prevalent privacy concerns, and arguably encourage states to act as laboratories for a national audience.[98] The current spectrum of experimental data laws may facilitate successful models for data protection.[99] However, this host of new laws poses multiple problems.[100] The myriad of different laws makes compliance challenging for Internet companies.[101] Also, states' efforts to protect personal data may be tempered by the online industry's aggressive lobbying.[102] California's current laws reflect this tug-of-war.[103] The state emerged as a leading advocate of consumer privacy rights by passing a "do-not-track" bill and criminalizing the online publication of identifiable nude photos.[104] But lobbying efforts brought down its third proposal, the "right-to-know" bill, which would have required businesses to disclose the consumer information they share with third parties.[105]

3. Constitutional Law

The Supreme Court has struggled to align constitutional notions of privacy with advancing technology.[106] The Fourth Amendment provides the battleground for fights over constitutional privacy issues.[107] It prohibits unreasonable searches and seizures and

---

95. Somini Sengupta, *No U.S. Action, So States Move On Privacy*, N.Y. TIMES, (Oct 31, 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html [http://perma.cc/7XH3-Z7NC].

96. *See id.*

97. *See id.*

98. *See id.*

99. *See id.*

100. *See id.*

101. *Id.*

102. *Id.*

103. *Id.*

104. *Id.*; *see also* CAL. BUS. & PROF. CODE § 22575 (2013), http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370 [http://perma.cc/3J3A-R68L].

105. *See* Sengupta, *supra* note 95

106. *See* Bedi, *supra* note 50, at 37.

107. *See id.*

protects the right of the people to be secure in their homes.[108] While the amendment aims to protect Americans' privacy, in *Olmstead v. United States*, the Court upheld the constitutionality of the government's warrantless wire-tapping because it did not invade the defendant's physical property.[109] Justice Brandeis, in a prescient dissent, said the Court must contemplate "not only of what has been but of what may be" when applying the Constitution.[110] He argued that the Fourth Amendment's language imbued the character of such protections, not their physical manifestations.[111] Someday, Brandeis warned, technology's advances may enable the government to expose intimate personal details without "removing papers from secret drawers."[112]

However, the Court's next major privacy decision, *Katz v. United States*, arguably eroded common-law trespassory protections by adding the "reasonable expectations test."[113] The Court held the Fourth Amendment did not protect a person's knowing, voluntary exposure of information in public, even in his home.[114] A person's subjective privacy expectations would warrant Fourth Amendment protection only if society recognized them as "objectively reasonable."[115]

But recent cases reflect the disconnect between emerging technology and a realistic, satisfying societal privacy standard.[116] In *Kyllo v. United States*, the Court confronted a case involving the government's warrantless thermal imaging of a suspect's home.[117] The Court held that the government eavesdropping constituted an unlawful search.[118] Justice Scalia echoed Brandeis's concerns, saying, "[I]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[119] Finally, in the landmark *United States v. Jones* decision, the Court returned to a property-based privacy approach, holding the government's warrantless use of a GPS tracker

---

108. *See* U.S. CONST. amend. IV.

109. Olmstead v. United States, 277 U.S. 438 (1928).

110. *See id.* at 473.

111. *See id.* at 477.

112. *Id.* at 474.

113. Katz v. United States, 389 U.S. 347 (1967).

114. *See id.* at 360.

115. *See id.* 361 (noting that the "reasonable expectations test" would calibrate individual privacy expectations with societal norms) (Harlan, J., concurring).

116. *See* Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

117. *Id.* at 29.

118. *Id.* at 40.

119. *Id.*

on the defendant's car an unlawful trespass.[120] Nonetheless, Justice Sotomayor criticized existing privacy jurisprudence.[121] In particular, she questioned the *Katz* premise that information disclosed to third parties does not deserve privacy protection.[122] Calling the premise "ill-suited to the digital age," Sotomayor highlighted the asymmetry between how much information individuals reveal to third parties in exchange for the mere "convenience" of completing daily tasks.[123] She further noted the tautology of relying on a societal norm for privacy expectations as technology pushes its "inevitable" diminution.[124]

C. "I'll Hold the Popcorn": Secondary Use Problems with the Third-Party Doctrine

Sotomayor's opinion crystallized the third-party doctrine's striking threat to personal privacy.[125] In today's digitized world, third parties have become default channels for moving and storing personal information.[126] Only a thin film separates third-party data brokers from the government, which can use its subpoena power to obtain personal information.[127] Given the illusory protection rendered to personal data, secondary data use seems even farther removed from meaningful protection.[128]

1. The Third-Party Doctrine

The third-party doctrine provides a corollary to the *Katz* "reasonable expectations" rationale for Fourth Amendment privacy.[129] The third-party doctrine asserts that a person has no reasonable expectations of privacy against the government if he voluntarily discloses information to a third party.[130] In *United States v. Miller*, the seminal third-party doctrine case, the Supreme Court held the

120. United States v. Jones, 565 U.S. ___, 132 S.Ct. 945, 949 (2012).

121. *See id.* at 957 (Sotomayor, J., concurring).

122. *Id.*

123. *Id.*

124. *Id.* at 962.

125. *See id.* at 957–58.

126. *See* Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 FL. COASTAL L. REV. 33, 67 (2011) ("Just because a person transmits information into cyberspace should not imply that the person has relinquished his or her right to privacy. . . . [L]ife in the twenty-first century occurs in cyberspace.").

127. *See* Brotherton, *supra* note 75, at 571 (stating that the third-party doctrine allows the government to circumvent the Fourth Amendment and go on legal "fishing expeditions"); *see also* Constine, supra note 53.

128. *See* Brotherton, *supra* note 75, at 575.

129. *See id.*

130. *See id.*

government's warrantless search of the defendant's financial records did not violate the Fourth Amendment.[131] The Court said the defendant had no reasonable expectations of privacy because he volunteered his financial information to a third party—his bank.[132] This indicates that a person's expectation that his information would be used for limited purposes does not shield him from government intrusion. [133]

The implications of the third-party doctrine are problematic for several reasons.[134] First, the third-party doctrine's premise is outdated.[135] In today's world, virtually all communications move across networks via third-party systems, such as Facebook and Google.[136] The third-party doctrine thus conflates the act of modern communication with "voluntary" relinquishment of one's information: in fact, there is no viable alternative.[137] Indeed, the third-party doctrine's origins evince its outmoded rationale.[138] The third-party doctrine bases its voluntary principle on a human context for information disclosure.[139] That is, critical to the "voluntary" element is the assumption that people share their information through other humans. The Supreme Court case *Smith v. Maryland* illustrates this flawed premise.[140] In the early days of the third-party doctrine, calling someone else meant passing personal information through a phone operator.[141] Thus, communicating through third parties required deliberate disclosure to another human being.[142] Making phone calls and sending mail carried the implicit risk that the person on the other end passing the information on to the sender might connect a lot of dots in Small Town, USA.[143] But the subsequent

131. *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).

132. *See id.*

133. *See* Brotherton, *supra* note 75, at 571.

134. *See* Ghoshray, *supra* note 126, at 73; Matthew Tokson, *Automation and the Fourth Amendment,* 96 IOWA L. REV. 581 (2011).

135. *See* Tokson, *supra* note 134, at 585.

136. *See* Ghoshray, *supra* note 126, at 73 (noting that "*Smith* held that there is one necessary condition to complete the communication--voluntarily disclosing such information to a third party. . . . The necessary condition I am referring to is the continued evolution of human existence.").

137. *See id.*

138. *See* Tokson, *supra* note 134, at 634.

139. *See id.*

140. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

141. *See* Tokson, *supra* note 134, at 585.

142. *See id.* at 600.

143. *See id.* at 615.

automation of third-party processes removes that meaningful and intentional assumption of risk.[144]

2. Beyond the Third-Party Doctrine: Other Privacy Arguments

Critics of the privacy movement have seized upon the third-party doctrine's continued life as evidence that society does not care about information privacy.[145] Since anti-privacy arguments also necessarily reject secondary data concerns, this Section will briefly address several prominent anti-privacy critiques.[146] First, critics argue that the mere disclosure of information carries an assumption of risk.[147] Willful disclosure negates privacy expectations because the act itself exposes information.[148] However, privacy advocates contend this argument distorts the idea of privacy.[149] Privacy is not binary.[150] Providing information to a selective circle of people, or in a designated forum, does not contemplate its complete public exposure.[151] To the contrary, limiting disclosure of information indicates the user intends to keep her data *within* certain bounds.[152]

Second, critics argue the current piecemeal privacy regime shows that society does not value privacy enough to enact stronger protections.[153] However, this argument does not account for behavioral fallacies that online privacy tends to invoke.[154] For instance, users tend to underestimate the potential risk of privacy harms. To them, the immediate gratification of using "risky" websites seems to outweigh the chance their personal information will be misused.[155] Websites prod users to accept these future risks by presenting them with lengthy privacy policies while trumpeting their

144. *See id.* at 582 (explaining that in the Fourth Amendment context, people assumed the risk that persons with whom people converse may reveal the information to others, yet "the information disclosed to these online third parties is generally not exposed to human beings at all; rather, it is processed entirely by automated equipment . . . However, courts have, without discussing the issue, already begun to treat automated Internet systems as the equivalent of human beings.").

145. *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, 223–26 (2012).

146. *Cf. id.*

147. *See* Brotherton, *supra* note 75, at 577.

148. *See* Ghoshray, *supra* note 126, at 74–75.

149. *See* Solove, *supra* note 76, at 535.

150. *See* Tokson, *supra* note 134, at 617.

151. *See* Solove, *supra* note 76, at 535.

152. *See id.*

153. *See* Ozer, *supra* note 145, at 223.

154. *See id.* at 226.

155. *See id.*

sites as "free."[156] These factors, coupled with the appeal and ease of "free" advertising, may persuade people to undervalue risks to their personal privacy.[157] Further, these individual fallacies contribute to the collective action problem that online privacy faces.[158] Framing privacy as an individual decision undermines the universal, interconnected nature of the issue.[159] Indeed, public polls belie the notion that consumers remain unconcerned about their online privacy and could possibly even be unaware of these issues.[160]

3. Secondary Data Use: What's the Harm, Really?

Critics contend that even if the current state of privacy law is problematic, it does not merit significant attention because privacy issues often do not evince actual harm.[161] Actual harm refers to traditional categories of tortious consequences, such as financial or physical damage.[162] However, online privacy harms pose intangible effects which may prove nonetheless devastating.[163] For example, potential harms posed by secondary data use include harms to dignity, power imbalances between the data holder and the data proprietor, and data misappropriation.[164] Secondary data use may seem less likely to pose privacy harms than interpersonal data because data brokers slice identifying information into bits.[165] However, secondary data use arguably threatens just as much information insecurity.[166] Data brokers do not sell secondary data in isolation.[167] Thus, even if secondary data is anonymized, research shows such disparate parts are easily de-anonymized.[168] For example, researchers reassembled anonymized Netflix data to reveal users' political and religious views

156. *See id.* at 225–26.

157. *See id.* at 223.

158. *See id.* at 224.

159. *See* Andrew Clement & Christie Hurrell, *Information/Communication Rights as a New Environmentalism*, COMPUTERIZATION MOVEMENTS AND TECHNOLOGY DIFFUSION: FROM MAINFRAMES TO UBIQUITOUS COMPUTING (2008).

160. *See* Ozer, *supra* note 145, at 222.

161. *See id.* at 228.

162. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY, 174–79 (Harvard University Press, 2008).

163. *See id.*

164. *See* Solove, *supra* note 76, at 487–90.

165. *See, e.g.*, Ozer, *supra* note 145, at 228 (explaining that "independently innocuous data points" can be aggregated in revealing ways because data brokers can retain disparate bits of individual information to form fuller profiles of them, which may de-anonymize them).

166. *See id.*

167. *See* Ozer, *supra* note 145, at 229.

168. *See id.*

just based on their movie histories.[169] In another study, one researcher used three public cross-reference points with the public census to uniquely identify 87 percent of the US population.[170] This researcher simply took the public anonymous data and combined people's five-digit ZIP codes with their sex and date of birth to uniquely identify specific people.[171]

Moreover, reaggregation of secondary data may distort third parties' impressions of user profiles.[172] Incomplete data sets heighten the risk that these inaccuracies may be manipulated.[173] In such instances, harm occurs regardless of whether or not damage results from specific instances of misuse.[174] The specter of secondary data manipulation threatens to have a chilling effect on personal behavior.[175] As people grow increasingly aware of the uncertain implications of secondary data, their understanding informs and inhibits behavior.[176] In sum, far from harmless, secondary data use threatens to erode basic freedoms if it remains unchecked.[177]

II. ANALYSIS

This Part divides analysis of secondary data solutions based on the onus for each solution.[178] Each Section is categorized by which entity or regime bears the responsibility of carrying out the privacy framework.[179] Section A discusses putting the onus on a social movement. Section B discusses putting the onus on federal law. Section C discusses putting the onus on the private industry. However, several proposals offer intriguing twists on traditional privacy frameworks by integrating principles from different sources.

---

169. *See id.* at 230.

170. *See* Ozer, *supra* note 145, at 229.

171. *See id.*

172. *See* Solove, *supra* note 76, at 482–84.

173. See *id.*

174. *See id.* at 482.

175. *See* Solove, *supra* note 76, at 559 ("[D]ecisional interference also resembles insecurity, secondary use, and exclusion. . . . [T]hese information-processing harms can have a chilling effect on a person's decisions regarding her health and body.").

176. *See id.*

177. *See id.*

178. Onus is defined as "[o]ne's duty or responsibility." OXFORD ENGLISH DICTIONARY, http://www.oxforddictionaries.com/us/definition/american_english/onus [http://perma.cc/B3DF-RXAW].

179. *See id.*

A. Social Movement

One proposed solution involves framing the privacy problem as a social movement.[180] The burden of this movement would fall on the privacy community to harness their collective resources to effectuate change.[181] Growing literature on social-movement theory focuses on using the environmental movement as starting reference.[182] This framework aims to leverage successful activism into a platform for permanent, sustainable access to power.[183]

There are several benefits to this approach.[184] First, the social movement works easily as a framing device because the burgeoning privacy movement shares many similarities with the environmental movement.[185] The Internet parallels an ecosystem because it contains a sphere of interconnected actors and systems.[186] Further, the ready similarities between online and offline ecosystems offer palpable metaphors to cohere difficult ideas about privacy.[187] Thus, proponents of this framework suggest that privacy advocates can adapt environmental movement's familiar concepts to articulate their own strategies.[188] For instance, viewing secondary data's potential harms as an externality may spur disparate strands of the privacy movement to unite as a stronger force for change.[189] Environmental activists galvanized public awareness by highlighting environmental disasters like oil spills and filing activist lawsuits against industry polluters.[190] Similarly, privacy advocates could rouse public alarm for secondary data misuse, decrying dangers posed by widespread hacking and suing repeat offenders.[191]

Critics argue the social movement framework does not provide a viable solution.[192] First, they contend data privacy concerns are not ripe for a social movement.[193] Privacy scholar Colin Bennett analyzed

---

180. *See* Cary Coglianese, *Social Movements and Law Reform: Social Movements, Law, and Society: The Institutionalization of the Environmental Movement*, 150 U. PA. L. REV. 85 (2001); *see also* Clement & Hurrell, *supra* note 159; Ozer, *supra* note 146, at 218.

181. *See* Clement & Hurrell, *supra* note 159, at 340.

182. *See, e.g., id.*

183. *See* Coglianese, *supra* note 180, at 87.

184. *See id.*

185. *See* Clement & Hurrell, *supra* note 159, at 17.

186. *See id.*

187. *See id.*

188. *See id.*

189. *See, e.g., id.* at 15.

190. *See* Coglianese, *supra* note 180, at 91.

191. *See id.*

192. *See* Ozer, *supra* note 145, at 232.

193. *See id.*

the emerging privacy community with social movement characteristics.[194] He concluded the privacy community lacked such essential features as a common focal point to rally the community for change.[195] Privacy means different things to different people.[196] Due to this lack of uniformity, privacy's variable definitions thus cut against mass mobilization.[197] Second, critics argue that episodic public alarm over national privacy incidents cannot sustain collective action.[198] Finally, the scale of the demand is daunting. Information "wants to be free."[199] The sheer volume of information released into the online ether poses complex tracking problems, making it difficult to hold sources accountable for discrete harms.[200]

B. Federal Law

1. Background

A second approach to addressing secondary data concerns puts the onus on the federal government. This approach elevates secondary data to the national forefront.[201] Though specific proposals differ, their general approach shares several characteristics. First, this approach aims to streamline secondary data processes in ethical, yet efficient, ways.[202] Second, this approach suggests that secondary data should be considered a "public good."[203] Acceptance—or perhaps resignation to—secondary data's widespread use accompanies this premise.[204] Thus, the approach seeks to balance concerns from

---

194. *See id.*

195. *See id.*

196. *See* Adam Thierer, *Privacy, Security, and Human Dignity in the Digital Age; The Pursuit of Privacy in a World Where Information Control is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 414 (2013) (citing Professor Daniel J. Solove's description of privacy as a "conceptual jungle").

197. *See id.*

198. *See* Ozer, *supra* note 145, at 232.

199. *See* Thierer, *supra* note 196, at 431.

200. *See id.*

201. *See* Charles Safran et al., *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper*, 14 J. AM. MED. INFORM. ASSOC., 1, 3 (2007).

202. *See* FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change*, F.T.C., 1, 44 (Dec. 2010) [hereinafter FTC Report] (proposing "commonly accepted data practices" for privacy), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, [http://perma.cc/QVM3-9W43].

203. *See* Safran et al., *supra* note 201, at 6; Sharona Hoffman & Andy Podgurski, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 SMU L. REV. 85, 90 (2012).

204. *See* Asay, *supra* note 78, at 335.

stakeholders on both sides of secondary data transactions. Third, the approach emphasizes education as a necessary corollary to the law's successful implementation.[205] Education legitimizes people's autonomy and empowers them to make informed decisions about secondary data.[206] Further, the educated public would serve as a democratic check on objectionable federal regulation and firm policies.[207] Finally, the approach is multifaceted.[208] Additional prongs supplement the proposed federal laws.[209] These prongs range from privacy principles to security safeguards.[210] Such models arguably reflect the complex nature of the challenges secondary data pose.[211]

2. Model Federal Law Proposal

For instance, scholar Clark D. Asay suggests a model federal law to address the current piecemeal regime.[212] This proposal provides the baseline of privacy safeguards that states have failed to achieve.[213] The law would invoke the notice-and-choice model to effectuate the safety mechanisms.[214] It focuses on holding companies accountable for third parties' secondary uses of consumer information.[215] Like California's Data Security Breach Act, the law would require companies to notify consumers if third parties used their data beyond the purposes for which it was intended.[216] The law would also require companies to disclose the third parties who use the secondary data.[217] Additionally, the law would provide consumers with a right of action to enforce their privacy rights.[218] However, the law's terms constrain its reach.[219] Per the law's definition, it would only apply to data termed "personally identifiable information"

---

205. *See* FTC Report, *supra* note 202, at 13; Hoffman & Podgurski, *supra* note 203, at 128.

206. *See, e.g.*, Hoffman & Podgurski, *supra* note 203, at 128.

207. *See id.* at 138–39.

208. *See id.* at 143.

209. *See id.*

210. *See, e.g.*, *id.* at 127.

211. *See, e.g.*, Deidre K. Mulligan & Jennifer King, *PRIVACY JURISPRUDENCE AS AN INSTRUMENT OF SOCIAL CHANGE: Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 1025 (2012).

212. *See* Asay, *supra* note 78, at 324.

213. *See id.* at 329.

214. *See id.* at 323.

215. *See* Mulligan & King, *supra* note 211, at 999–1000.

216. CAL. CIV. CODE § 1798.82 (2015).

217. *See* Asay, *supra* note 78, at 340.

218. *See id.* at 351.

219. *See, e.g.*, *id.* at 341 ("[D]isclosures of non-PII could still result in some subjective privacy harm for consumers . . . .").

(PII).[220] So, the law would exclude potential PII that had been aggregated and anonymized.[221]

Similarly, President Obama recently contributed his own proposed model law to this approach.[222] In a speech introducing the law, President Obama explained, "Each of us as individuals have a sphere of privacy around us that should not be breached, whether by our government, but also by commercial interests."[223] Though details are still emerging, the law's framework sounds similar to Asay's proposed model law.[224] Called the Personal Data Notification and Protection Act (PDNPA), this law aims to begin fixing the patchwork of privacy laws by providing a national baseline of privacy standards.[225] Like the model law, the PDNPA works through an accountability mechanism to achieve this goal, requiring companies to notify consumers of data breaches within a specified time.[226] However, PDNPA seems to focus on reacting to primary data breaches, not secondary data issues.[227]

3. HIPAA as Alternative Model Law

An alternative source for federal law comes from an extant framework, the Health Insurance Portability and Accountability Act (HIPAA). HIPAA provides an infrastructure of laws, policies, and best practices to protect personally identifiable healthcare records.[228] The rapid rise of unregulated secondary data use in the healthcare sector has prompted scholars to label the secondary data mining industry an "urgent" concern.[229] While the merits of facilitating limited secondary data use is beyond the bounds of this Note, the healthcare industry's insights on secondary data may offer innovative ways to confront its complex issues.

---

220. *See id.*

221. *See id.*

222. Michael D. Shear & Natasha Singer, *Obama to Call for Laws Covering Data Hacking and Student Privacy*, N.Y. TIMES, (Jan. 11, 2015), http://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?_r=0 [http://perma.cc/5RDE-4YS4].

223. *See id.*

224. *See id.*; *see, e.g.*, Asay, *supra* note 78, at 324.

225. *See* Shear & Singer, *supra* note 222.

226. *See id.*; *see, e.g.*, Asay, *supra* note 78, at 322.

227. *See* Shear & Singer, *supra* note 222 (explaining other components to the speech included proposing measures to prevent collection of such information as school data, home energy data, and credit scores).

228. *See* Hoffman & Podgurski, *supra* note 203, at 95.

229. *See* Safran et al., *supra* note 201.

HIPAA's current privacy safeguards provide the groundwork for secondary data protections.[230] HIPAA organizes healthcare information into a taxonomy of confidentiality categories. A "safe harbor" provision ensures data is anonymized before potential disclosure to third parties, cabined by a statistical standard that determines risk of re-identification.[231] Additionally, HIPAA requires breach notifications for certain types of information and offers an outside governmental mechanism, the Office of Civil Rights, as a means of enforcement.[232]

This HIPAA-based framework aligns national standards to create a multitiered model for secondary data.[233] To start, this approach would shift the law's focus from a notice-and-choice model to a notice-and-education model.[234] Advocates of this model argue that pivoting from "choice" to "education" provides a more meaningful, realistic balance between consumer autonomy and secondary data's upsurge.[235] By fostering public dialogue and transparency about secondary data practices, advocates hope to engender sufficient public trust to implement a meaningful consent system.[236] In turn, the public's newfound familiarity with the privacy spectrum could facilitate greater flow of information through secondary data's regulated use.[237] New, more nuanced consent systems would render the current broad-based privacy options obsolete.[238] A series of external checks would reinforce privacy protections and unify expectations for handling secondary data access, use, and misuse.[239] These include a national set of working definitions for secondary data and regular auditing by independent security experts.[240]

This enhanced HIPAA-inspired model could offer several advantages. First, streamlining secondary data could promote its efficient use for public service.[241] For example, researchers could analyze the data to ward off epidemics through early detection.[242]

---

230. *See, e.g.*, *id.* at 5.

231. *See* Hoffman & Podgurski, *supra* note 203, at 96, 130.

232. *See id.* at 138.

233. *See, e.g.*, Safran et al., *supra* note 201, at 4.

234. *See* Hoffman & Podgurski, *supra* note 203, at 139 (arguing that educating data subjects about records-based research concerns should replace requiring their consent for inclusion in health studies).

235. *See, e.g.*, *id.* at 138.

236. *See id.* at 138–40.

237. *See id.*

238. *See* Asay, *supra* note 78, at 333 (criticizing the "blanket opt in/opt out system").

239. *See* Hoffman & Podgurski, *supra* note 203, at 91.

240. *See id.* at 102.

241. *See* FTC Report, *supra* note 202, at 13.

242. *See* Hoffman & Podgurski, *supra* note 203, at 127.

Second, educating the public arguably lends agency to choices about personally identifiable information.[243] As such, offering a spectrum of consent options validates the public's understanding of secondary data with third party use by aligning access on both sides.[244] Finally, perhaps the HIPAA-inspired model's greatest advantage stems from its overarching, multifaceted approach to secondary data.[245] By offering a flexible set of tools, the approach reflects and responds to the complex demands of secondary data concerns.[246]

However, the HIPAA-based approach to secondary data use confronts several problems. First, this approach may be limited by preexisting confines.[247] Suggestions for dealing with HIPAA-related secondary data command a deep, perhaps insular, focus on a specialized industry.[248] Further, these suggestions are not just healthcare specific, but supplemental provisions to HIPAA's original laws.[249] Thus, applying HIPAA's secondary data standards to broader commercialized secondary data may prove inappropriate and unpredictable.[250] Second, the proposals may suffer irrelevance from technology's rapid advances.[251] Secondary data exchange has already outstripped the legal and ethical procedures in place.[252] It is unclear whether even a multifaceted filter of controls would be able to keep up.[253] Finally, this model may fail to provide sufficient reliability and protection for personally identifiable information.[254] Critics of de-identification have argued that a variety of commercial stakeholders possess an overriding interest in obtaining salient consumer data.[255] Similarly, new consent options may prove just as illusory as the old ones;[256] potential permission requests for secondary

243. *See, e.g.*, *id.* at 141.

244. *See, e.g.*, *id.*

245. *See id.* at 143.

246. *See id.*

247. *See, e.g.*, Asay, *supra* note 78, at 326 (citing industry-specific federal sectorial laws in the current privacy regime).

248. *See id.*

249. *See, e.g.*, Safran et al., *supra* note 201, at 5 (proposing to fill the gaps in HIPAA's current infrastructure); *see also* Ayres, *supra* note 57, at 1019 (proposing a model law to expand HIPAA's static privacy rules).

250. *See* Asay, *supra* note 78, at 325.

251. *See* Brotherton, *supra* note 75, at 581.

252. *See id.*

253. *See id.*

254. *See id.* at 561.

255. Examples of interests which may override these ethical concerns include an insurer's interest in the insured's health records and a blackmailer's in the target's financial records. *See id.*; *see also* Hoffman & Podgurski, *supra* note 203, at 104.

256. *See* Brotherton, *supra* note 75, at 582.

data may be too complex to effectively administer so far in advance.[257] These issues may render de-identification procedures ineffectual at keeping secondary data out of inappropriate hands.[258]

C. Industry

A third approach to secondary data protection puts the onus on the companies that use it.[259] Tasking the problem's source with its solution makes intuitive sense, in a way.[260] Advocates of this approach start with the simple premise that companies should "do better."[261] Also, advocates insist privacy controls constitute a basic tenet of doing business—companies should take reasonable steps to protect consumer privacy because such measures are integral to basic customer relations.[262]

Privacy by design offers one prominent example of a private sector solution. This is a process guided by a set of values, the Fair Information Practice Principles (FIPP).[263] Put another way, privacy by design is a systematic approach to embedding privacy into the underlying architecture of any technology.[264] Per FIPP, this approach seeks to integrate privacy as a core technology component.[265] In doing so, this approach seeks to make privacy a prerequisite instead of an afterthought.[266] Privacy by design has several possible advantages. First, it is proactive.[267] To comply with FIPPs, companies would have to embed privacy into the underlying architecture of their products.[268] Demanding front-end privacy changes could bolster privacy's parallel evolution with technology's advances.[269] Indeed, studies show that integrating privacy during the design phase is more efficient and less

257. *See, e.g.*, Hoffman & Podgurski, *supra* note 203, at 121 (explaining that some future medical research projects probably involve too much speculation about information use for present meaningful consent).

258. *See id.* at 103.

259. *See* Ira S. Rubinstein, *Technology: Transforming the Regulatory Endeavor: Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1414 (2011).

260. *See id.*

261. *See, e.g.*, Mulligan & King, *supra* note 211, at 1028 ("[C]ompanies have an obligation to attend to consumers' understandings of the normal rules of engagement during online interactions and that if they want to deviate and capture novel information they must 'clearly and prominently disclose' and gain consent . . . .").

262. *See* Rubinstein, *supra* note 259, at 1455.

263. *See id.* at 1418.

264. *See id.* at 1411–12.

265. *See id.* at 1420–21.

266. *See id.*

267. *See id.* at 1431.

268. *See id.* at 1412.

269. *See id.* at 1426; *see also* Ayres, *supra* note 57, at 976.

costly than resolving security issues later on.[270] Second, it is flexible.[271] Unlike federal law requirements, which may prove unwieldy or rote for key industry players, the approach allows companies to customize privacy applications to their particular technologies and audiences.[272] Further, this flexible approach may facilitate privacy innovations.[273] Advocates of privacy by design have pointed out that assigning the privacy challenge to the technology sector complements their privileged role in society.[274] Because they are the chief architects of the current environment riddled with privacy issues, they are well-positioned to craft a more privacy-protective version.[275] Moreover, the steps they take to improve privacy protections may produce positive secondary effects on corresponding issues. For example, industry-wide adoption of privacy by design principles would foster commonly accepted data practices.[276] The universal nature of such best practices facilitates consumer trust.[277] In turn, such consumers' coherent expectations could promote more meaningful choices about consent.

But this approach suffers from several drawbacks. First, the technology industry has been slow to adopt it.[278] Without more urgent pressures, it is unclear how or when the approach would crystallize into efficacy.[279] Second, privacy by design is costly.[280] It often requires companies to reverse their default privacy schemes, which consumes time, research, and money.[281] Further, no resounding evidence shows heartier privacy controls would offer companies any competitive advantage.[282] Indeed, to the contrary, secondary data's booming industry attributes its success to the *lack* of privacy controls.[283] In totality, financial disincentives to create meaningful privacy protections feed the self-perpetuating cycle of doubt over privacy's

---

270. *See* Rubinstein, *supra* note 259, at 1426.

271. *See, e.g.*, FTC Report, *supra* note 202, at 44 (suggesting companies incorporate privacy design throughout the life cycles of their products and services).

272. *See id.*

273. *See* Rubinstein, *supra* note 259, at 1453.

274. *See* Mulligan & King, *supra* note 211, at 991.

275. *See id.*

276. *See, e.g.*, FTC Report, *supra* note 202; *see also* Ayres, *supra* note 57, at n.295; Rubinstein, *supra* note 259, at 1440 (linking the diminished trust from privacy breaches to the potential loss of consumers).

277. *See id.*

278. *See* Rubinstein, *supra* note 259, at 1412.

279. *See id.*

280. *See id.* at 1443.

281. *See id.*

282. *See id.* at 1436.

283. *See id.* at 1439–40.

commercial viability.[284] The lack of privacy research is reinforced by the lack of apparent financial incentive to invest in it, and so the self-perpetuating cycle spirals into market failure.[285] Finally, privacy by design may not produce the universal outcomes that its advocates ideate.[286] The approach may be too amorphous to translate into concrete, consistent privacy practices.[287] Companies may also prove too skittish or burdened by competing financial stakes to police the bounds of their world.[288] Thus, the fallacies of self-regulation arguably amplify privacy by design's potential inconsistencies.[289]

These potential shortcomings have not stopped scholars from proposing solutions to address the private sector's potential market failures. For instance, one healthcare scholar suggests seizing upon the private sector's financial motives to craft a compromise between third parties and consumers regarding secondary data use.[290] This proposal would use a subscription model for secondary data.[291] The subscription model would revolve around a self-regulated federation of networks.[292] Third parties would pay the federation to subscribe to and use pre-filtered data the federation aggregated.[293] Such a system could financially sustain the secondary data industry while protecting consumers' sensitive data.[294]

Alternatively, data scholar Ira S. Rubinstein has suggested remedying current privacy market failures with a coregulatory approach.[295] Rubinstein argues this approach combines necessary regulatory controls to address privacy's market failures while retaining sufficient flexibility to spur innovation.[296] The approach retains this flexibility through a variety of possible legal tools.[297] These options range from agency rulemaking, which requires industry input, to safe harbor provisions, which would exempt companies from certain privacy regulations if they were granted the opportunity to explore experimental privacy solutions.[298]

---

284. *See, e.g., id.*
285. *See id.*
286. *See id.* at 1421.
287. *See id.*
288. *See id.* at 1445.
289. *See id.*
290. *See* Hoffman & Podgurski, *supra* note 203, at 120.
291. *See id.* at 139.
292. *See id.*
293. *See id.*
294. *See id.*
295. *See* Rubinstein, *supra* note 259, at 1451.
296. *See id.*
297. *See id.* at 1451–52.
298. *See id.* at 1452.

An intriguing twist to the coregulatory approach by scholars Deidre K. Mulligan & Jennifer King proposes deriving privacy principles from the growing field of Human Computer Interaction (HCI).[299] HCI focuses on individual control and humans' interpersonal boundaries to shape a dynamic view of privacy.[300] HCI relies on user context for effectiveness.[301] This paradigm thus places the user, rather than the information, at the center of the privacy inquiry.[302] In doing so, HCI aims to craft privacy models that reflect normative user experiences.[303] Individuated privacy models could offer accurate, sensitive bounds amenable to optimal user interaction.[304]

III. SOLUTION

Putting the responsibility on any single entity threatens to perpetuate the shortcomings that first propagated the unregulated secondary data market.[305] Yet left untouched, secondary data's continued proliferation may result in irreparable privacy infringements on people's lives.[306] Given the urgent and latent nature of the secondary data problem, the federal government should implement a two-fold tactic.[307] Following Rubinstein's lead, a coregulatory approach involving both federal law and the private sector should be adopted.[308] A coregulatory approach would provide the most potent, feasible solution to this complex issue.[309] At the most basic level, the federal law would provide three components that build off each other: (1) a guiding premise, (2) a basic framework for minimum secondary data privacy standards modeled off the guiding premise, and (3) sanctions to enforce the standards.[310] The private

299. *See* Mulligan & King, *supra* note 211, at 993.

300. *See id.* at 1019.

301. *See id.* at 1022.

302. *See id.* at 1023.

303. *See id.* at 993.

304. *See id.* at 1023.

305. *Cf.* Rubinstein, *supra* note 259, at 1443.

306. *See, e.g.*, Ayres, *supra* note 57, at 971.

307. *See* Rubinstein, *supra* note 259, at 1445.

308. *See id.*

309. *See id.*

310. This approach is inspired by a convergence of the aforementioned frameworks. Representative inspirations for the three-component formula include: *cf.* Shear & Singer, *supra* note 222 ("[W]e want a federal baseline, and leave the states with the freedom to establish stronger standards.") (quoting Marc Rotenberg, the president of the Electronic Privacy Information Center). *See generally* FTC Report, *supra* note 202 (privacy should be the default setting); Asay, *supra* note 78 (federal law and sanction system suggested); Mulligan & King; *supra* note 211 (HCI principles as underlying guidance); Rubinstein, *supra* note 260 (minimum federal standards to allow flexibility for firms to adapt).

sector would complement federal law by crafting solutions based off the federal scheme.[311] The guiding premise would follow user-centric HCI principles rather than contract principles, lending the model a flexible, normative framework.[312]

As previously discussed, privacy models often rely on a central premise to anchor their frameworks. Unlike previously discussed models, however, this proposed privacy model would invoke HCI principles to guide its framework.[313] Models that focus on contract theories are ineffectual because they reduce privacy decisions to rigid, law-focused constructs.[314] Most humans are not lawyers.[315] Furthermore, privacy is not bilateral.[316] Thus, the human-centric principles of HCI vastly improve upon existing privacy models by seeking to adapt privacy preferences to users, rather than the other way around.[317] Based on HCI principles, then, the federal law model would work off the following simple premise: privacy is the default, and the user is the focus.[318]

A. Framework

This central premise translates into an intuitive, user-based privacy model.[319] Called the "Signal Model," it derives from the ubiquitous traffic signal system.[320] The Signal Model allows the user to allocate her data permissions with three privacy "signals."[321] These privacy signals dictate third-party permissions. Each privacy signal corresponds to a traffic light color and its requisite meaning. The green "Go" signal means the user allows third parties to use all data. The red "Stop" signal means third parties do not have permission to use any of the data. The yellow "Caution" signal means the data use is context-specific and the user could release permissions on the data depending on the situation. While the scope of data subject to the Signal Model would have to be determined, ideally the user could

311. *See generally* Rubinstein, *supra* note 259.

312. *See generally* Mulligan & King, *supra* note 211.

313. *See generally id.*

314. *See* Brotherton, *supra* note 75, at 567.

315. *See Legal Profession Statistics*, AM.BAR ASS'N, http://www.americanbar.org/resources_for_lawyers/profession_statistics.html [http://perma.cc/KA6F-AGQ8].

316. *See generally* Solove, *supra* note 76.

317. *See generally* Mulligan & King, *supra* note 211.

318. *See generally id.*

319. *See generally id.*

320. *See generally id.*

321. *See, e.g.*, Asay, *supra* note 78, at n.158 (citing studies suggesting food labels aid consumers in providing meaningful notice and information to improve their choices).

apply the Signal Model to whatever groups of data that website offers. Potential data categories could include particular data outcomes users wanted to exclude or particular categories of information.[322]

Critics of the Signal Model would likely question whether this system translates into realistically customizable controls.[323] After all, the Signal Model may not adequately target the variable nature of secondary data permissions.[324] In this way, the Signal Model's permission system may not sufficiently equate the user's understanding of what she permits data brokers to use with the data broker's understanding of what or how it can use the data.[325] While this is an understandable concern, it is arguably inevitable: at some point, virtually any consent system, no matter how granular, will not capture a subset of user privacy.[326] Further, if companies implemented these heightened privacy frameworks, they would probably pass on the increased costs to consumers.[327] The Signal Model is meant to provide a feasible starting point, not an end solution, to address these perpetual challenges.[328] Further, this may be an optimal role for the federal government to take on, with ongoing education and a reliable sanctioning system to alleviate concerns about distortion between permission and use.[329] Namely, the federal government could appoint the FTC to facilitate education and sanctions for this new model, as the FTC has analogous experience implementing other regulatory frameworks.[330]

The Signal Model offers several advantages. First, it adheres to HCI's context-dependent, individualistic approach to privacy.[331] Each user has a different idea of what privacy means, what types of personal information she is willing to share, and what ways she is willing to share it.[332] The Signal Model gives each user the

322. *See* Hoffman & Podgurski, *supra* note 203, at 121.

323. *See* Mulligan & King, *supra* note 211, at 1022.

324. *See id.*

325. *See, e.g.*, Asay, *supra* note 78, at 324.

326. *See* FTC Report, *supra* note 202, at 55 (suggesting a limited set of data practices be addressed through privacy by design).

327. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 20 (2000).

328. *Cf.* Asay, *supra* note 78, at 324.

329. *See, e.g.*, Rubinstein, *supra* note 259, at 1451.

330. *See id.* at 1446 (citing the FTC's experience as a regulatory actor to support its enforcement role in a co-regulatory approach, including such sanctioning methods as pursuing strategic cases); FTC Report, *supra* note 202, at 14 (describing the FTC's role in educating technology and business companies on privacy issues through such efforts as public roundtables, whitepapers, and workshops).

331. *See* Mulligan & King, *supra* note 211, at 1022.

332. *See id.*

opportunity to completely individuate and protect her personal information based on how she values it.[333] The intuitive appeal of aligning data choices with traffic lights makes the process easy to use.[334] At the same time, the Signal Model offers the technology industry a universal set of expectations to expedite its ability to incorporate corresponding privacy features.[335] Finally, this universal system facilitates the federal government's enforcement of privacy violations. Breaches of the system would be highlighted by any data broker's explicit exploitation of "red" data and possibly "yellow" data. Meanwhile, the yellow signal acts as a safe harbor mechanism for users and third parties by rendering its corresponding secondary data use context-specific.[336] Whereas before data brokers had little incentive to negotiate with their ostensible sources of income, now yellow signal data could drive third parties and their primary data counterparts to come up with innovative solutions, negotiating with users in exchange for this data.[337] Though the framework's mechanisms for implementation and use are beyond this Note, the Signal Model offers a robust, universal baseline for leveraging secondary data use into a mutually agreeable exchange while protecting user privacy.

IV. CONCLUSION

Secondary data use thrives in the legal gray area that underpins the Internet's troves of personal data. However, as scholars and Supreme Court justices have pointed out, people's general ignorance about technology's implications for secondary data does not ratify its use. The inconclusive nature of studies concerning personal privacy values, coupled with the asymmetrical incentives between data brokers and users, supports treatment of secondary data as a market failure. However, any singular approach to resolving this market failure would likely fall short, as the three entities most qualified to confront the issue have encountered their own obstacles in doing so. And the current patchwork of state privacy laws, varied self-regulatory efforts, and niche federal laws offer inconsistent protection to a universal threat of irreparable and far-reaching privacy harms. The Signal Model offers a practical coregulatory approach to safeguard personal data while aligning incentives between third

333. *See id.*

334. *Cf. id.*

335. *See generally* FTC Report, *supra* note 202.

336. *See, e.g.*, Rubinstein, *supra* note 259, at 1452 (suggesting safe harbors to preserve flexibility for companies to negotiate standards with the federal government).

337. *See id.*

parties and users. While designing an effective rollout mechanism for engaging users in the Signal Model poses an initial challenge, the Signal Model itself would provide sufficient, simple guidance for the federal government to regulate data brokering. Though it remains to be seen, education about secondary data may produce user reticence to assign third-party data permissions in any capacity. Yet this potential side effect of secondary data regulation arguably offers technology companies precisely the opportunity to innovate that its current unregulated use lacks. Companies could vie for users' attention by offering economic or access incentives in exchange for data under the green "Go" or yellow "Caution" signals. Thus the coregulatory approach, by proposing to fit data permissions to user needs, has the potential to pioneer privacy changes into a viable commercial industry.

Kelsey L. Zottnick[*]

* J.D. Candidate, Vanderbilt University Law School, 2016; B.A., Rice University, 2011. The author wishes to thank her parents, Kerry and Lynn Zottnick, as well as her siblings, for their unwavering support. The author would also like to thank Josh Sureck and Victoria Roessler for their patience, valuable feedback, and senses of humor throughout this process. In addition, the author would like to thank Danielle Drago, Danielle Dudding, and the staff of the VANDERBILT JOURNAL OF ENTERTAINMENT & TECHNOLOGY LAW for their hard work and help. Finally, the author would like to thank Erin Shackelford for her advice and encouragement, without which the author would not have submitted this Note for publication.