University of Michigan Journal of Law Reform

Volume 49 | Issue 3

2016

Protecting Personal Information: Achieving a Balance between User Privacy and Behavioral Targeting

Patrick Myers
University of Michigan Law School

PROTECTING PERSONAL INFORMATION: ACHIEVING A BALANCE BETWEEN USER PRIVACY AND BEHAVIORAL TARGETING

Patrick Myers*

Websites and mobile applications provide immeasurable benefits to both users and companies. These services often collect vast amounts of personal information from the individuals that use them, including sensitive details such as Social Security numbers, credit card information, and physical location. Personal data collection and dissemination leave users vulnerable to various threats that arise from the invasion of their privacy, particularly because users are often ignorant of the existence or extent of these practices. Current privacy law does not provide users with adequate protection from the risks attendant to the collection and dissemination of their personal information. This Note advocates a comprehensive solution: a federal statute that introduces a contractual mentality to encourage informed consent to companies' data collection and dissemination practices.

Table of Contents

* J.D. Candidate, 2016, University of Michigan Law School; B.A., 2013, University of Michigan.

INTRODUCTION

Between February and May of 2015, a criminal organization stole personal financial information from over 100,000 individuals off of the Internal Revenue Service's (IRS) website, which it then used to claim tax refunds under several of those individuals' names.[1] That data also allowed the criminal organization to open bank accounts and credit lines, and claim additional tax refunds.[2] The criminals then used that personal information, which included Social Security numbers, birth dates, and physical addresses, to request taxpayers' forms.[3] They also answered the victims' personal identity verification questions, which enabled them to steal more sensitive financial information, such as salary data and individuals' taxpayer deductions.[4] This was particularly troubling considering that the victims would have expected the IRS to adequately protect their privacy. These large-scale data breaches, accomplished with users' personal information, have become increasingly common in recent years.

The advent of modern technology has changed how people go about their lives. They stay connected through social media, conduct business online, and on the whole, expedite their daily activities. Smartphones and other mobile devices, in particular, allow access to these abilities at all times. Many users are unaware that the benefits they derive from this technology come at the expense of their privacy. Companies have exploited the ubiquity of Internet usage through the collection and dissemination of users' personal information. But, these practices also provide many advantages to users such as efficient, personalized online experiences through behavioral marketing and advertising. They also yield a significant source of profits for companies not only through targeted advertising, but also from the tangible value of aggregated personal information.

Unfortunately, these practices pose serious risks to users' privacy. Besides an invasion of privacy, the collection and dissemination of personal information can result in identity theft, financial fraud, discrimination, and even physical harm. Users are not fully informed of these risks because of the flawed nature of user agreements and inadequate consent to privacy policies. Companies' data collection and dissemination practices are outlined in their

1. Jose Pagliery, *Criminals Use IRS Website to Steal Data on 104,000 People*, CNN MONEY (May 26, 2015), http://money.cnn.com/2015/05/26/pf/taxes/irs-website-data-hack/.

2. *Id.*

3. *Id.*

4. *Id.*

privacy policies, which are often written in lengthy, complex legalese. Users often miss these policies, which are typically located on a separate page of a website or application (app). Many users view agreeing to a company's privacy policy as an obstacle to their online activity, simply clicking "I Agree" without reading the agreement.

This Note describes the current practices surrounding the collection and dissemination of personal information, examining the benefits and drawbacks to both users and companies. Taking the interests of users and companies into account, this Note seeks to develop a solution that will adequately protect individual privacy without disrupting the everyday use of technology. Part I explains the mechanics of collecting and disseminating user information, along with its attendant benefits and risks. Part II discusses the currently applicable law and its shortcomings in addressing the problems laid out in Part I. Part III proposes a comprehensive statutory remedy that strikes a balance between user privacy and company interests.

I. MECHANICS, COSTS, AND BENEFITS OF COLLECTING AND DISSEMINATING USER INFORMATION

The collection and dissemination of personal information is now a pervasive component of users' online experiences. This Part will explore the mechanics of how companies and third parties collect and disseminate users' information. It will also examine the advantages and disadvantages that these practices create for both users and companies.

A. Mechanics of Collection and Dissemination

Websites and mobile applications collect users' personal information by using several methods. The most common (and visible) approach is to compile information through forms.[5] On many websites and apps, users consciously enter personal information such as names, addresses, phone numbers, and employment details.[6] This represents a fairly straightforward way for companies to gather personal information. Not all data collection, however, is apparent to

5. Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 563 (2008).

6. *Id.*

the user. In addition to this conscious distribution, users may unwittingly give up personal information just by visiting the site or app.

When a user visits a website, it may place "cookies," small data files, on a visitor's browser to allow the site to identify the user on his or her next visit to the site.[7] The next time that user visits the website, the cookies relay the relevant information to the site owner.[8] In so doing, cookies make Web browsing more efficient for the user and the website; for example, users can stay logged in to a site rather than entering their login information each time they visit a new page.[9] Websites also use cookies to track browser history.[10] The combination of cookies and referrer information, which provides websites with the last URL visited by the user, allows site owners to track the sites visited by any given user.[11]

In addition to placing their own cookies on users' browsers, websites frequently allow third parties, such as online advertisers, to do the same.[12] These third parties use cookies to track users' browsing history and assemble profiles of each user.[13] Third party companies can also purchase personal information collected through forms, cookies, or other methods, from the websites that users visit.[14] The collection and dissemination practices of these third parties create various privacy concerns, particularly since users are unaware of the identities and purposes of those entities. This lack of knowledge vitiates any explicit or implicit consent on the part of the users.

Recently, companies have started to move away from using cookies and have begun to employ other methods to track users' activities and collect their information.[15] This is because cookies have become less effective in the face of browser settings that allow users to limit or block cookies.[16] People also increasingly use mobile

---

7. Luke J. Albrecht, *Online Marketing: The Use of Cookies and Remedies for Internet Users*, 36 SUFFOLK U. L. REV. 421, 422 (2003).

8. Stephanie A. Kuhlmann, *Do Not Track Me Online: The Logistical Struggles over the Right "To Be Let Alone" Online*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 229, 235 (2011).

9. *See id.*

10. *See* Albrecht, *supra* note 7, at 422.

11. Jay P. Kesan & Rajiv C. Shah, *Deconstructing Code*, 6 YALE J. L. & TECH. 277, 299 (2004).

12. *See* Raizel Liebler & Keidra Chaney, *Google Analytics: Analyzing the Latest Wave of Legal Concerns for Google in the U.S. and the E.U.*, 7 BUFF. INTELL. PROP. L.J. 135, 139 (2010).

13. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1409–10 (2001).

14. *See* Ciocchetti, *supra* note 5, at 581.

15. *See* Brian Boland, *Facebook Exec: Cookies Don't Cut It Anymore for Online Ad Measurement; Why the Industry Needs to Replace Cookies With People*, ADVERTISING AGE (Mar. 21, 2014), http://adage.com/article/digitalnext/cookies-cut-anymore-online-ad-measurement/292225/.

16. Olga Kharif, *The Cookies You Can't Crumble*, BLOOMBERG BUSINESSWEEK (Aug. 21, 2014), http://www.businessweek.com/articles/2014-08-21/facebook-google-go-beyond-cookies-to-reap-data-for-advertisers.

devices, most of which do not allow applications to utilize cookies.[17] Advertisers have adapted to these changes by using other methods such as "people-based" measuring,[18] which allows companies to keep track of users' activities across different devices, such as computers, tablets, and mobile phones.[19] These alternate methods present their own advantages and disadvantages. Although alternate methods offer more effective behavioral advertising, they may also be more difficult for users to disable, potentially making anonymous browsing impossible.[20]

Companies typically inform individuals of data collection and dissemination by detailing such practices in their terms and conditions. Usually, companies urge users to accept their terms and conditions before browsing their sites and using their services.[21] Often, the mode of acceptance is to click an "I accept" button. Some websites and apps do not require explicit acceptance, but rather state their terms and conditions on a separate page.[22] Adding further complication, websites' and apps' terms and conditions are often written in lengthy, complex legalese.[23] Notwithstanding the privacy issues these practices implicate, which will be discussed later, it is questionable whether these user agreements effectively notify visitors about data collection and dissemination practices. In fact, many users view the acceptance of terms and conditions as an obstacle to their online activity, not explicit consent to compile and sell their personal information.[24] Although the contract law principle that failure to read an agreement is no excuse[25] may have some merit, the methods by which websites and apps obtain consent are intrinsically flawed. And in the case of third-party cookies, consent is arguably nonexistent.

---

17. *Id.*

18. *See* Boland, *supra* note 15.

19. *See* Adit Abhyankar, *Continued Growth of Cross-Device Advertising and Other 2015 Predictions*, PERFORMANCEIN (Dec. 29, 2014), http://performancein.com/news/2014/12/29/continued-growth-cross-device-advertising-and-other-2015-predictions/.

20. *See* Kharif, *supra* note 16.

21. *See* Ciocchetti, *supra* note 5, at 561.

22. *See id.* at 586.

23. *See id.* at 587–89.

24. *See id.* at 561.

25. *See, e.g.*, 27 SAMUEL WILLISTON, WILLISTON ON CONTRACTS § 70:113 (4th ed. 1990) ("A party is not excused from a contract simply for not having read the agreement before signing and accepting its benefits. The failure to read an agreement . . . is no excuse for pleading ignorance of the contents of the unread contract.").

B. Benefits to Users and Companies

The collection and dissemination of personal information can be mutually beneficial for both individuals and companies. One major benefit is a personalized and efficient Internet browsing experience. Because websites place cookies on visitors' browsers, it allows the sites to recognize each person the next time he or she visits. These first-party cookies are commonly used by e-commerce companies for identification purposes.[26] Websites originally employed cookies to facilitate the now-familiar online shopping cart, which stores customers' item selections as they browse an e-commerce site.[27] First-party cookies offer a more efficient online experience by allowing websites to register user activity. Without cookies, every visit to a webpage would be treated as the user's first, "like visiting a store where the shopkeeper had amnesia."[28] In short, cookies provide users with a personalized and efficient browsing experience and enable websites to take note of these preferences.

Data collection and dissemination also result in tailored marketing and advertising for Internet users. E-commerce businesses, such as Amazon, can record a user's browsing history across multiple sites and advertise based on his or her preferences. Third-party tracking methods, such as cookies, allow companies with whom the user is not interacting to similarly monitor online activity and tailor advertisements. Websites can also disseminate user information to enable third parties to target their advertisements. Facebook, for example, uses information that members provide to advertise for other companies.[29] This behaviorally targeted advertising creates benefits for consumers and businesses—consumers see products related to their individualized interests—which helps make online shopping more efficient. They may also discover new interests based on their activities and purchases. Businesses, for their part, can directly market to individuals, exposing consumers to products for which they are actively shopping and also to related products they may not have been considering. Moreover, companies can change their websites based on personal information to improve user experiences.[30] For instance, news services such as *The Washington Post* and *Reuters* offer personalized websites or apps that show

26. *See* Ciocchetti, *supra* note 5, at 565.
27. *See* Kesan & Shah, *supra* note 11, at 298–99.
28. John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. TIMES, Sept. 4, 2001, at A1.
29. *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/advertising (last visited Jan. 3, 2016).
30. Liebler & Chaney, *supra* note 12, at 142.

news stories relevant to each individual subscriber, taking into account personal interests, articles a person has read in the past, and location.[31] Companies may also modify promotions to accommodate aggregate consumer trends.[32]

Due to tailored marketing and advertising, companies and third parties derive significant economic benefit from collecting and distributing users' personal information. As discussed above, businesses extract value from observing market trends, and more specifically, by aggregating personal information.[33] Compiling personally identifiable information benefits businesses because "it raises the probability that advertising will translate into sales, and it cuts the expense of advertising to uninterested consumers."[34] Data collection therefore facilitates a cost-efficient advertising model that is increasingly necessary to remain competitive.[35]

In addition to these benefits from tailored marketing and advertising, the collection of personal information can produce further economic gains through its dissemination. Companies amass individual profiles which include information such as "education levels, occupation, height, weight, political affiliation, ethnicity, race, hobbies, and net worth."[36] These digital "dossiers" are commonly and freely sold to other companies.[37] As a consequence of each of the aforementioned strategies, businesses can realize concrete economic benefits from gathering and selling users' personal information within the bounds of any applicable privacy laws.

---

31. *See* Russell Adams, *Paper Starts New Website*, THE WALL STREET JOURNAL (Feb. 11, 2011), http://www.wsj.com/articles/SB10001424052748704265604576136120092550768; Eric Blattberg, *Reuters TV Aims to Personalize News Broadcasts*, DIGIDAY (Nov. 11, 2014), http://digiday.com/publishers/reuters-tv/. For another example of companies using personal information to enhance user experience, see Kathleen Chaykowski, *Facebook Shakes Up News Feed in Push to Show More Relevant Videos*, FORBES (June 29, 2015), http://www.forbes.com/sites/kathleenchaykowski/2015/06/29/facebook-shakes-up-news-feed-in-push-to-show-more-relevant-videos/ (describing how Facebook tracks its members' actions related to videos in their news feed—such as whether they turned on the volume or watched them in full screen—to determine what videos they will see and where in their feed the videos will appear).

32. Kuhlmann, *supra* note 8, at 236–37.

33. John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Pii") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 1, 10 (2009).

34. *Id.* at 9.

35. *Id.* at 10.

36. Solove, *supra* note 13, at 1409–10.

37. Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 970 (2003).

C. Privacy Concerns and Drawbacks

Although the collection and dissemination of personal information produces benefits for both users and companies, these practices also give rise to several disadvantages, including privacy concerns. The invasion of a person's privacy is primarily an intangible harm, which makes it difficult to quantify.[38] But, companies' data collection and dissemination practices also create certain tangible risks in the form of identity theft, financial fraud, and physical harms.

As mentioned above, users may not be aware of, or consent to the compilation and distribution of their personal information. Evidence indicates that Internet users do not read a site's terms and conditions,[39] but rather click "Accept" in order to move on to their intended online activity. Even if some users are aware that websites compile their personal information, they may underestimate the extent to which it is collected and used.[40] Without full knowledge of the intrusions of their privacy, users cannot effectively safeguard against attendant financial or physical harms.

Privacy concerns are particularly salient when third parties are involved. When users enter personal information into Web forms, they acknowledge that the sites are collecting their data. It is usually not apparent from websites' disclosures, however, that the sites may sell this data to third parties.[41] This is because third-party data collection does not involve direct consent on the part of the user.[42] Even if the collection by or dissemination to third parties is disclosed in a website's terms and conditions, the purported consent is attenuated. Most users do not read websites' or apps' privacy policies, which means that companies sell users' personal information without their knowledge or explicit consent.[43] These aspects of personal data collection undermine the legitimacy of the entire practice. They call into question whether the goals of convenience,

---

38. *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1808 (2010).

39. *See* Rebecca Smithers, *Terms and Conditions: Not Reading the Small Print Can Mean Big Problems*, THE GUARDIAN (May 11, 2011), http://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems (reporting a survey of British Web users that showed only seven percent read online terms and conditions before accepting); *see also* Jakob Nielsen, *How Little Do Users Read?*, NIELSEN NORMAN GROUP (May 6, 2008), http://www.nngroup.com/articles/how-little-do-users-read/ (citing an empirical study demonstrating that, on average, Web users only read about twenty percent of the words on a Web page).

40. *See* Ciocchetti, *supra* note 5, at 574–75.

41. *See id.* at 578.

42. *See id.*

43. *See id.*

efficiency, and economic benefits for users and companies justify the (sometimes nonconsensual) methods of data compilation and distribution.

One prevalent concern is that aggregating user information increases the risk of identity theft and financial fraud. Although disclosing individual pieces of information may not present a strong possibility of identity theft, the gathering of data into digital profiles intensifies this threat.[44] For instance, although an identity thief could not accomplish much with an email address, he could potentially cause severe financial harm by hacking into a bank account if he combined the individual's email address, Social Security number, and mother's maiden name. Although a user may take extensive steps to avoid sharing information with any one site that is sufficient for identity theft, aggregation circumvents precautionary measures.

The danger of identity theft is further compounded if companies do not take adequate measures to protect users' data. And unfortunately, the frequency of large-scale data breaches has risen in recent years.[45] Several corporations with broad consumer bases have fallen victim to breaches involving the theft of the sensitive personal information of millions of people.[46] Taken in context of the pervasive collection and dissemination of personal information, these breaches present a serious threat to consumer privacy, as well as to businesses' competitive advantage. First, data breaches expose consumers to a material risk of identity fraud.[47] Users cannot effectively safeguard against this privacy concern because their data may be sold to almost any entity.[48] Therefore, users cannot take appropriate precautions to ensure that only companies zealously guarding their personal information have possession of it. In other cases, users cannot avoid giving up that data because entities such

---

44. *See id.* at 575–76.

45. Elise Viebeck, *FBI: Data Breaches "Increasing Substantially,"* THE HILL (May 14, 2015), http://thehill.com/policy/cybersecurity/242110-fbi-official-data-breaches-increasing-substantially.

46. *See, e.g.*, Paul Ziobro & Danny Yadron, *Target Now Says 70 Million People Hit in Data Breach*, WALL STREET JOURNAL (Jan. 10, 2014), http://www.wsj.com/articles/SB10001424052702303754404579312232546392464 (discussing how up to seventy million people were affected by Target's data breach, which involved the theft of information such as debit and credit card accounts, names, mailing addresses, phone numbers, and email addresses); Malathi Nayak, *U.S. FCC Imposes $25 Million Fine on AT&T Over Customer Data Breach*, REUTERS (Apr. 8, 2015), http://www.reuters.com/article/2015/04/08/us-at-t-settlement-dataprotection-idUSKBN0MZ1XX20150408 (noting that around 280,000 AT&T customers were affected by a data breach which involved disclosure of names, Social Security numbers, and other account information).

47. *See* Soma et al., *supra* note 33, at 11.

48. *See id.* at 581.

as the IRS require people to disclose it. The IRS theft discussed earlier shows the extent of the financial risks to which individuals are exposed, particularly when a company does not sufficiently protect its users.[49] Second, these large-scale data breaches affect businesses, as the failure to protect personal information may cause consumers to use other services instead.[50] Large-scale data breaches demonstrate how hackers may exploit the practices of gathering and distributing personal information and thereby simultaneously harm a significant number of users.

In addition to financial harms, the collection and dissemination of personal information can also result in "physical harm, blackmail, discrimination, and emotional or mental distress from embarrassment."[51] Since digital profiles are readily available for sale, any interested party can purchase an individual's personal information.[52] This has resulted in criminal cases in which the perpetrator gained access to the victim's whereabouts.[53] Further, there is a risk of employment discrimination when employers discover employees' personal information, and users may also suffer from mental distress or embarrassment from the public disclosure of sensitive information.[54] For instance, a group of hackers targeted the website Ashley Madison in July of 2015 and released sensitive personal details about thirty-one million users, including their email addresses, residences, and sexual preferences.[55] These potential abuses of possessing another's personal information exemplify the risks of companies collecting and disseminating user data.

---

49. *See supra* Introduction; *see also, e.g.*, Brianna Ehley, *Watchdog: IRS Ignored Warnings Before Getting Hacked*, THE FISCAL TIMES (June 2, 2015), http://www.thefisc altimes.com/ 2015/06/02/Watchdog-IRS-Ignored-Warnings-Getting-Hacked ("[T]he IRS had failed to act on a handful of recommendations the [Treasury Inspector General for Tax Administration] had previously made to address serious security weaknesses within the agency's databases.").

50. Charles Arthur, *Sony Suffers Second Data Breach with Theft of 25m More User Details*, THE GUARDIAN (May 3, 2011), http://www.theguardian.com/technology/blog/ 2011/may/03/ sony-data-breach-online-entertainment.

51. Kuhlmann, *supra* note 8, at 241.

52. *See* Ciocchetti, *supra* note 5, at 581.

53. *See, e.g.*, U.S. v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010) (upholding the conviction of a former Social Security Administration employee under the Computer Fraud and Abuse Act for accessing the personal information of seventeen people for nonbusiness reasons); Robert O'Harrow, Jr., *Online Firm Gave Victim's Data to Killer*, CHICAGO TRIBUNE (Jan. 6, 2002), http://articles.chicagotribune.com/2002-01-06/news/0201060305_1_pretexting-docu search-amy-boyer (reporting how a woman was murdered by a former classmate who purchased her personal information online).

54. *See* Kuhlmann, *supra* note 8, at 246.

55. Dina Spector, *A 'Cheating' Husband Reveals What it Feels Like to be Exposed in the Ashley Madison Hack*, BUSINESS INSIDER (Sept. 2, 2015), http://www.businessinsider.com/ what-it-feels-like-to-be-exposed-in-ashley-madison-data-breach-2015-9?r=UK&IR=T (describing a husband and wife's experience after their personal information was leaked).

Although collecting and disseminating personal information creates benefits for both users and companies, the concerns and potential abuses that the practice raises warrants some manner of protection. At the core of these harms is that users, who have the greatest incentives to protect their information, are not fully aware of the risks of data collection and dissemination. Companies' privacy policies do not adequately notify users, and users usually do not recognize the significance of privacy policies. Websites and apps "generally [only] have to follow privacy policy procedures in order to avoid legal trouble," rather than to ensure that users understand and consent to such procedures.[56] Large-scale data breaches aggravate this consumer information gap, indicating that popular companies are not taking adequate measures to protect customers' sensitive information. And, in light of the ubiquitous practice of selling personal data, users cannot depend on websites or apps to protect sensitive information.

D. Intensified Need for Comprehensive Protection in Light of Modern Technology

It is particularly important for Congress to provide today's users with comprehensive protection because emerging user trends toward mobile browsing exacerbate the drawbacks of collecting and disseminating personal information. Since 2007, global mobile usage has quadrupled, surpassing global desktop usage, which also rose steadily during the same time period.[57] According to one report, "nearly one-fifth of cell owners (17%) use their cell phone for most of their online browsing."[58] This trend warrants renewed consideration of federal, all-encompassing consumer privacy protection laws, because mobile browsing presents more acute risks for users.

Mobile devices provide companies with valuable information, such as "contact numbers, location, and a unique identifying number that cannot be changed or turned off."[59] Because of this valuable data and the recent trends in mobile application usage,

---

56. Ciocchetti, *supra* note 5, at 581.

57. Danyl Bosomworth, *Mobile Marketing Statistics 2015*, SMART INIGHTS (July 22, 2015), http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics.

58. Jan Lauren Boyles et al., *Privacy and Data Management on Mobile Devices*, PEW RESEARCH CENTER (Sept. 5, 2012), http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

59. Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 296 (2012).

behaviorally targeted advertisements will increasingly focus on mobile users. Due to the ubiquity of smartphones and similar mobile devices, it is paramount that consumers fully comprehend the privacy policies of the applications they browse. For example, a significant number of popular mobile applications recently disseminated "user phones' unique device IDs to third parties without the users' awareness or consent."[60] Such a lack of knowledge prevents users from proactively taking precautions to avoid the distribution of personal data to undesirable third parties. Given the rise in mobile usage, the widespread data collection and dissemination practices of apps are particularly troubling. According to a recent study, the overwhelming majority of apps, both paid and free, exhibit behaviors that threaten users' privacy.[61] These "risky behaviors . . . included location tracking, accessing the device's address book or contact list, single sign-on via social networks, identifying the user or the phone's unique identifier (UDID), in-app purchases, and sharing data with ad networks and analytics companies."[62]

Although web-based browsing presents similar risks, mobile devices amplify the dangers of data aggregation and distribution. For instance, the potential for physical harm increases if the perpetrator knows the exact location of his or her victim, as opposed to only a home address or place of employment.[63] Mobile devices can provide such information—and many do—since most people carry their phones with them at all times.[64] One recent study found that apps almost continually track a person's location: for instance, the Facebook app checked a user's location more than once per minute.[65] A default app on a Google Android phone "checked a user's location one million times in one month."[66] In addition to these practices, new people-based marketing methods make it almost impossible for users to maintain their privacy and safeguard sensitive

60. *Id.* at 297.

61. Neil McAllister, *How Many Mobile Apps Collect Data on Users? Oh . . . Nearly All of Them*, THE REGISTER (Feb. 21, 2014), http://www.theregister.co.uk/2014/02/21/appthority_app_privacy_study/ ("95 per cent of the top 200 free apps for iOS and Android exhibited at least one risky behavior. But so did 80 per cent of the top 200 paid apps, meaning pretty much all apps should be considered suspect.").

62. *Id.*

63. *See supra* Part I.C.

64. Tene & Polonetsky, *supra* note 59, at 296–97.

65. Chris Smith, *The Amount of Personal Data Some Android Apps Collect is Absolutely Shocking*, BGR (Dec. 17, 2014), http://bgr.com/2014/12/17/android-apps-personal-data-and-location/ ("The Google Play Store tracked a user's phone 10 times per minute at certain times.").

66. *Id.*

personal information.[67] In part, this is because mobile technology is a more recent development; users are not as well-versed in how to prevent companies from collecting and disseminating their personal information. Although some Web users may know how to disable cookies, they likely cannot translate these prevention techniques to their mobile devices. Even when users take steps to avoid tracking, their apps can still circumvent these measures.[68] In some cases, users might not be able to disable applications' collection and dissemination practices.[69] Users must, therefore, rely on legal protections to insulate themselves from the problems created by the collection and dissemination of their personal information.

II. SHORTCOMINGS OF APPLICABLE LAW

Currently, there is no uniform legal response to these issues. Although members of Congress have introduced several bills, no federal law directly addresses the problems discussed in Part I. This Part examines the legal concerns related to companies' collection and dissemination of users' personal information. It also considers the nature and extent of legal protections available to users: tort and contract law remedies, several proposed statutes that Congress did not enact, existing statutes with limited applicability, and Federal Trade Commission (FTC) regulatory efforts.

A. Legal Notions of Privacy

The concept of privacy has permeated American jurisprudence for over a century. In 1888, Judge Thomas M. Cooley articulated the quintessential legal definition of privacy as "the right to be let alone."[70] Several years later, Samuel Warren and Louis Brandeis announced a common law right to privacy in their influential (and aptly named) article, *The Right to Privacy*.[71] They posited that this

67. *See* Kharif, *supra* note 16.

68. *See* Peter Sayer, *Android Apps Exploit Permissions to Access Personal Info, Researchers Find*, INFOWORLD (Dec. 15, 2014), http://www.infoworld.com/article/2859565/mobile-technology/android-apps-exploit-permissions-to-access-personal-info-researchers-find.html ("One of the few options users have to avoid this tracking is a switch in the "Google Settings" app to reset their phone's advertising ID. That's not much help, though, as apps have other ways to identify users.").

69. *See* Kharif, *supra* note 16.

70. THOMAS M. COOLEY, THE LAW OF TORTS 29 (2d ed. 1888).

71. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

right was necessary to preserve a person's private and domestic life.[72] Warren and Brandeis argued that the right to be let alone had become a socially recognizable necessity on par with the right to own property and protections against bodily injury.[73] This individual right arose from a broader principle of privacy, separate from principles of contract or private property.[74] Brandeis described the right to privacy as "the most comprehensive of rights and the right most valued by civilized men."[75] The Supreme Court has recognized this foundational principle, interpreting the U.S. Constitution to guarantee personal privacy in certain circumstances such as in the home, in religion, and in private speech.[76] In *Griswold v. Connecticut*, the Supreme Court acknowledged that the constitutional right to privacy is "legitimate."[77]

Professor William Prosser described four separate torts for the invasion of a person's privacy: (1) intrusion upon the seclusion of another; (2) appropriation of another's name or likeness; (3) public disclosure of private facts; and (4) publicity which places another in a false light before the public.[78] These torts, while dissimilar, are all based on "the right to be let alone."[79] Most states have adopted these invasion of privacy torts through common law or statutes.[80]

Despite the ostensible availability of privacy tort law remedies, courts have imposed certain requirements that limit the feasibility of these remedies in protecting against companies' collection and dissemination of personal information. Many courts have not recognized privacy rights in voluntarily disclosed information, unless the information contains confidential characteristics or implicates a fiduciary relationship.[81] Courts have also looked at an individual's

---

72. *See id.* at 195.

73. *Id.* at 193–95.

74. *Id.* at 213.

75. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

76. *See, e.g.*, U.S. CONST. amends. I, IV. These guarantees do not protect a person from invasions of privacy by private parties. *See also*, Walter v. United States, 447 U.S. 649, 656 (1980).

77. Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

78. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

79. *Id.*

80. *See* PRIVACILLA.ORG, THE PRIVACY TORTS: HOW U.S. STATE LAW QUIETLY LEADS THE WAY IN PRIVACY PROTECTION 19–24 (2002), http://www.privacilla.org/releases/Torts_Report.pdf (listing exemplary cases, statutes, and other sources from each state that illustrate that state's approach to privacy tort protection).

81. Kuhlmann, *supra* note 8, at 233.

expectation of privacy in evaluating whether his or her privacy was invaded.[82]

Common law privacy torts cannot adequately protect against the collection and dissemination of personal information.[83] As one commentator noted, "[a]dvances in the technology of surveillance and the recording, storage, and retrieval of information have made it either impossible or extremely costly for individuals to protect the same level of privacy that was once enjoyed."[84] In the context of websites and mobile apps, users arguably have relinquished their privacy expectations.[85] Users voluntarily disclose personal information in many instances.[86] Furthermore, when a person uses a website or app, he or she either explicitly or implicitly agrees to a company's terms and conditions.[87] Since these agreements inform users of personal information collection and dissemination practices, they have vitiated their expectation of privacy.

One concern with this conclusion is that terms and conditions already raise issues of informed consent,[88] so whether a user can give up an expectation of privacy in this way is debatable. Another concern is that even users who are conscious of collection and dissemination risks will struggle to fully insulate themselves from ceding their expectation of privacy. As discussed above, new methods such as people-based marketing may make anonymous browsing impossible.[89] Unlike cookies, these techniques cannot be disabled by users.[90] Accordingly, users will be forced to sacrifice the convenience of modern technology, such as tablets and mobile devices, in exchange for their privacy. Given the pervasiveness and

---

82. *See, e.g.*, Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 374 (D.N.J. 2012) (holding that a woman "may have had a reasonable expectation that her Facebook posting would remain private, considering that she actively took steps to protect her Facebook page from public viewing"). The court described consistent case law on two ends of the privacy spectrum: "there is *no* reasonable expectation of privacy for material posted to an unprotected website that anyone can view," while "there *is* a reasonable expectation of privacy for individual, password-protected online communications." *Id.* at 373.

83. *See* Citron, *supra* note 38, at 1809.

84. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 465 (1980). This concern is even more prevalent 35 years later, with all of the technological improvements that have occurred in the interim. *See, e.g.*, Kharif, *supra* note 16.

85. See Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. TIMES (Jan. 9, 2011), http://www.nytimes.com/2011/01/10/technology/10privacy.html ("Last year, for example, the Justice Department argued in court that cellphone users had given up the expectation of privacy about their location by voluntarily giving that information to carriers.").

86. *See* Ciocchetti, *supra* note 5.

87. *See id.* at 561, 586.

88. *See supra* Part I.C.

89. *See* Kharif, *supra* note 16.

90. *See id.*

necessity of these technologies, online activity will likely come at the expense of a person's expectation of privacy.

The collection and dissemination of a person's personal information controverts this fundamental value of privacy, a principle essential to society that has been recognized by legal scholars for over one hundred years.[91] This value, however, is not only recognized by legal scholars. The Supreme Court has also affirmed the legitimacy of the right of privacy.[92] To secure this right, U.S. common law has provided several torts to protect individuals against the invasion of their privacy.[93] Although well-intentioned, these privacy torts do not adequately safeguard users from the collection and dissemination of their personal information.

B. Limited Reach of Contract Law

In essence, the interaction between a user and an online provider (whether a website or a mobile application) is a contractual agreement: an exchange of online services for something of value from the user. The user's contribution may be monetary, such as a subscription to a website or app, or intangible, in the form of his or her personal information.[94] With the development of the Internet and its role in commerce, online transactions with standard boilerplate contracts have become increasingly prevalent.[95] Courts have applied traditional contract law principles to these transactions.[96] A standard principle of contract law is that "a party may be bound by an instrument which he has not read."[97] Application of these traditional principles to the online context, however, may not always be appropriate. For example, two general types of online agreements implicate the problems raised by lack of informed user consent:[98] click-wrap and browse-wrap agreements.

A "click-wrap agreement" prompts the user to click an on-screen button to indicate that he or she has read the terms and conditions

91. *See* Warren & Brandeis, *supra* note 71, at 193–95.

92. Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

93. *See* Prosser, *supra* note 78, at 389.

94. *See* Soma et al., *supra* note 33, at 9–10.

95. Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577, 577 (2007).

96. *See generally* Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429 (2002).

97. John D. Calamari, *Duty to Read: A Changing Concept*, 43 FORDHAM L. REV. 341, 341 (1974).

98. *See supra* Part I.C.

and assents to the agreement.[99] These agreements are usually used in connection with software licenses. Courts have almost universally upheld the validity of click-wrap agreements, "settl[ing] on a mechanical assent analysis that only seeks to determine whether or not the 'I Agree' button was indeed clicked."[100] In the few instances that courts have refused to enforce the terms of click-wrap agreements, the analysis did not hinge on whether clicking a button was assent to a contract.[101] In a "browse-wrap agreement" a user, simply by visiting or using a website, agrees to be bound to the website's terms and conditions.[102] For these agreements, there is no active manifestation of assent.[103] Courts, however, have not drawn much of a distinction between click-wrap and browse-wrap agreements, resulting in the broad enforcement of both.[104] For such online contracts, courts look at whether a user had actual or constructive notice of the terms and whether he or she then assented to them; usually only unconscionable provisions are struck down.[105]

While contract law does provide a baseline, it applies only where there is an actual transaction. When a user is simply browsing a website and the website uses cookies to collect personal information, there is an exchange of that information for services that courts do not view as a contractual agreement. The few cases where courts have invalidated browse-wrap agreements share one common feature: "a point in time that the court could specifically identify as the moment when notice should have been provided, such as completing a sale . . . or downloading software."[106] It is therefore difficult for courts to find a lack of actual or constructive notice for typical Web or mobile use.[107] In the context of websites and mobile apps collecting and disseminating personal information, users only have a resort to contractual remedies when there is an egregious lack of notice or a provision that violates public policy.[108] Despite the similarity of privacy policies to contracts,

---

99. Michelle Garcia, *Browsewrap: A Unique Solution to the Slippery Slope of the Clickwrap Conundrum*, 36 CAMPBELL L. REV. 31, 35 (2013).

100. Davis, *supra* note 95, at 598.

101. *Id.* at 582 ("Instead, these courts either refused to enforce the agreements because there was insufficient evidence of clicking, or voided the terms based on traditional contract doctrines.").

102. Garcia, *supra* note 99, at 35–36.

103. *See id.* at 36.

104. *Id.* at 55.

105. *See* Davis, *supra* note 95, at 583.

106. Garcia, *supra* note 99, at 55.

107. *See id.*

108. *See* Davis, *supra* note 95, at 583.

"contract law . . . plays hardly any role in the protection of information privacy, at least vis-à-vis websites with privacy policies."[109] Accordingly, users whose personal information has been unknowingly collected or disseminated must hope that statutory or regulatory mandates govern their situation.[110]

C. Statutory Protections and Failed Legislative Attempts

There is no comprehensive federal statutory scheme that directly addresses the problems created by the collection and dissemination of users' information. For the most part, Congress has left this matter to the discretion of the FTC. In recent years, however, Congress has attempted to address these issues on several occasions, none of them successful. In 2011, Representative Jackie Speier introduced the Do Not Track Me Online Act.[111] This statute would have authorized the FTC to set standards for a user opt-out function, which would have allowed online users to prevent companies from collecting or disseminating their personal information.[112] The Act protected personal data such as a user's name, government identification numbers, financial and medical information, race, religious affiliation, and sexual orientation.[113] Covered entities were obligated to comply with a user's decision to employ the Do Not Track mechanism.[114] The Act further required companies to disclose their current information collection and dissemination practices to users. It also created a civil cause of action where state attorneys general could sue on behalf of resident users to prevent further violations, ensure compliance, or impose civil penalties.[115] The Act did not cover entities storing information from fewer than 15,000 individuals, as long as the entities did not (1) collect information on more than 10,000 individuals during a twelve month period, (2) "collect or store sensitive information," and (3) "use covered information to study, monitor, or analyze the behavior of individuals as

109. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 596 (2014) ("Contract law litigation theories have barely been attempted, as the number of cases involving these theories has been exceedingly low over the past fifteen to twenty years after the rise of privacy policies.").

110. *See* Juliet M. Moringiello & William L. Reynolds, *From Lord Coke to Internet Privacy: The Past, Present, and Future of the Law of Electronic Contracting*, 72 MD. L. REV. 452, 477 (2013).

111. Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011).

112. *Id.* § 3.

113. *Id.* § 2.

114. *Id.* § 3(a).

115. *Id.* § 5.

[their] primary business."[116] Although privacy advocates supported the Act, it faced opposition from the advertising industry and died in committee.[117]

In 2011, Senators John Kerry and John McCain proposed the Commercial Privacy Bill of Rights Act to "establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission."[118] The bill would have required covered entities to provide users with clear notice and an explanation of their information collection practices.[119] Although it would have provided users with an opt-out choice for data collection and dissemination, it did not allow for a Do Not Track mechanism.[120] The bill also prohibited a private cause of action, leaving enforcement to the FTC and state attorneys general.[121] Unlike the Do Not Track Me Online Act, this bill received support from businesses and the advertising industry and criticism from consumer and privacy advocates.[122] Despite having bipartisan support, this bill also died without a vote in Congress.

In 2013, Representative Hank Johnson introduced the Application Privacy, Protection, and Security Act of 2013 (APPS Act).[123] This Act required mobile apps to receive permission from users before collecting data, explain their collection and dissemination practices, and allow users to request that apps delete their data.[124] This proposal was significant because it was the first federal statute that would have applied to mobile applications. It would have provided app users with significant protection and a certain amount of control over apps' use of their data. The proposal had several drawbacks, however, as it applied only to apps, leaving websites unregulated.[125] It was also unfavorable to advertising companies,

---

116. *Id.* § 2(2).

117. *See* Wendy Davis, *Privacy 'Track Bill' Draws Key Support*, MEDIAPOST (Feb. 11, 2011), http://www.mediapost.com/publications/article/144858/ (detailing support from privacy advocates and critiques from advertising industry representatives).

118. 157 CONG. REC. S2387 (daily ed. Apr. 12, 2011).

119. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 201 (2011).

120. *See infra* Part II.D.

121. S. 799 §§ 403, 405(b)(1), 406.

122. *See* Cecilia Kang, *Senators Introduce Internet Privacy Bill*, THE WASHINGTON POST (April 12, 2011), http://www.washingtonpost.com/blogs/post-tech/post/senators-introduce-internet-privacy-bill/2011/04/12/AFL0CjRD_blog.html (reporting that the bill garnered support from Microsoft, Intel, and eBay, although consumer advocacy groups felt it did not provide enough protection to users).

123. H.R. 1913, 113th Cong. (2013).

124. *Id.*

125. *See id.*

which preferred self-regulation.[126] The APPS Act had a problematic safe harbor, "in which a company could be shielded from liability by following a code of conduct developed through the NTIA multistakeholder process, even though the requirements of that code of conduct may fall far below the substantive requirements of the APPS Act."[127] This safe harbor might have negated the effectiveness of the statute because companies could circumvent the protections of the Act. The APPS Act also died in Congress.

Congress has succeeded in providing additional protection for one specific situation: when companies collect children's personal information.[128] The Children's Online Privacy Protection Act (COPPA), passed in 1998, gives the FTC authority to issue regulations and enforce the provisions of the statute.[129] COPPA prohibits websites and online services from collecting a child's (a person under the age of thirteen) personal information unless they comply with the provisions of the Act.[130] COPPA requires the operator of the website or online service to provide notice of how the company collects and uses information, in addition to operator disclosure practices.[131] The operator must obtain verifiable parental consent for the collection, use, and dissemination of the child's information.[132] The operator is also prohibited from conditioning any activity, such as participating in a game or receiving a reward, on the child disclosing more personal information than is "reasonably necessary to participate in such activity."[133] COPPA also requires the operator to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[134]

Congress has also included privacy provisions in other statutes to protect specific types of information held by certain entities. The Gramm-Leach-Bliley Act requires financial institutions to give consumers privacy notices detailing the institutions' information-

126. *See* Jim Edwards, *Congress's New 'Apps Act' Could Change How You Use Your Mobile Phone Forever*, BUSINESS INSIDER (Jan. 18, 2013), http://www.businessinsider.com/the-apps-act-2013-1.

127. Daniel Parisi, *Mobile App Privacy: Developing Standard and Effective Privacy Tools for Consumers*, 15 N.C. J.L. & TECH. ON. 240, 260 (2014).

128. *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 et. seq.

129. *Id.* § 6505(a).

130. *Id.* § 6502(a).

131. *Id.* § 6502(b)(1)(A).

132. *Id.*

133. *Id.* § 6502(b)(1)(C).

134. *Id.* § 6502(b)(1)(D).

sharing practices and allow consumers to opt out of certain disclosures to nonaffiliated third parties.[135] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes a privacy rule that regulates the use and disclosure of protected health information.[136] While these statutes provide some degree of protection, no federal bills have been enacted that comprehensively address digital privacy concerns.

Although no federal statute protects all users from the privacy concerns discussed above, California passed a law that provides users with protection from the harms presented by companies' collecting and disseminating their personal information. The California Online Privacy Protection Act (CalOPPA) mandates that any company that collects users' personal information must conspicuously post its privacy policy.[137] A company's privacy policy must explain what personal information is collected, and list all third parties with whom the company shares the data.[138] Recent amendments, which went into effect on January 1, 2014, also require companies to disclose "how the operator responds to Web browser 'do not track' signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information."[139] In addition, companies must disclose whether third parties can collect users' information "over time and across different Web sites when a consumer uses the operator's Web site or service."[140]

CalOPPA is the most comprehensive online privacy statute, providing transparency for users. Unlike COPPA it protects all online users, not just children. CalOPPA allows California users to make fully informed, conscientious decisions about what online services to use and what information they are comfortable with disclosing. The law is also broad enough to encompass modern technologies, protecting users who use multiple devices.[141] CalOPPA does have

---

135. *See* The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq. The Act does allow financial institutions to disclose consumers' personal information "to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services." *Id.* § 6802(b)(2).

136. *See* The Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-1, et seq. The HIPAA Privacy Rules are codified at 45 C.F.R. 164.

137. California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575 et. seq.

138. *Id.* § 22575(b)(1).

139. *Id.* § 22575(b)(5).

140. *Id.* § 22575(b)(6).

141. *See* Jane Hils-Shea, *California's Do-Not-Track Law Presents Challenges to Online Businesses*, FROST BROWN TODD LLC (Oct. 14, 2013), http://www.frostbrowntodd.com/resources-1619.html.

some shortcomings, however. It does not, for instance, create a private cause of action.[142] The statute also does not require companies to honor a user's choice not to be tracked.[143] Despite these drawbacks, this law is a major step toward providing users with effective privacy protection against companies' collection and dissemination of personal information, although it is only effective in California.

D. FTC Regulatory Activity

The FTC oversees the implementation and operation of nongovernmental privacy policies.[144] The agency has the authority to penalize companies for "not adhering to their own publicized privacy policies."[145] Under the Federal Trade Commission Act, the FTC may sue companies for engaging in unfair or deceptive practices.[146] Therefore, if a company does not comply with its own privacy policy or if the policy is misleading, it may be subject to FTC enforcement. The FTC can fill in the statutory gaps in the user privacy field; even though there is no comprehensive federal scheme, the FTC has jurisdiction under the FTC Act over any "person, partnership, or corporation" that engages in these practices.[147]

One paradigmatic example of FTC enforcement action is *F.T.C. v. Toysmart.com, LLC*, in which the FTC sued a company that sold customers' personal information to third parties in contravention of the company's privacy policy.[148] Toysmart collected personal information such as names, addresses, shopping preferences, and data about consumers' children, and sold it to third parties.[149] Ultimately, the court ordered third parties in possession of the consumers' personal information to delete all data and comply with COPPA.[150] The FTC successfully brought suit, although COPPA only applied to some of the data—the information was mostly from adult consumers.[151] Despite COPPA's limited applicability to this case, the FTC had jurisdiction under the FTC Act and could protect

---

142. *Id.*

143. *AB370: California's "Do Not Track" Law*, COOLEY LLP (Oct. 8, 2013), http://www.cooley.com/ab370-californias-do-not-track-law.

144. *See* Liebler & Chaney, *supra* note 12, at 162.

145. *See* Kuhlmann, *supra* note 8, at 234.

146. *See* FTC Act, 15 U.S.C. §§ 52–53.

147. *Id.* § 53(a).

148. F.T.C. v. Toysmart.com, LLC, No. 00-11341-RGS, 2000 WL 34016434, *1 (D. Mass. July 21, 2000).

149. *Id.*

150. *Id.* at *2.

151. *See id.* at *1; Press Release, FTC, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), https://www.ftc

the users' personal information because of Toysmart's failure to adhere to its privacy policy.[152] This case demonstrates how the FTC can provide protection even when a statute does not directly cover all users.

The FTC has also recommended a Do Not Track mechanism, which would allow users to make a uniform decision to prevent companies from tracking their online activity. The "most practical method . . . would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements."[153] This would offer several advantages, such as built-in privacy for online activity, simplified choice, and increased transparency.[154] The FTC's recommendation offers more protection to users, but it is not mandatory for online service providers. Companies also are not required by law to respect a user's desire not to be tracked, unless they state otherwise in their privacy policies.[155] The drafters of the Consumer Privacy Bill of Rights Act of 2011 declined to include such a mandate; Senator Kerry asserted that a Do Not Track requirement would have upset the balance of consumer and industry support.[156] More problematically, this function may be more difficult to implement for mobile devices. As discussed above, behavioral advertisers are moving away from using cookies and are instead utilizing people-based marketing, which is harder for users to disable.[157]

Despite the agency's efforts, FTC regulation in this field cannot provide adequate protection to users from the various concerns related to collection and dissemination of their personal information. The FTC has jurisdiction under the FTC Act only when a company engages in unfair or deceptive practices.[158] The agency therefore cannot require completely transparent company practices as

---

.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding.

152. *See id.* at *2; Kuhlmann, *supra* note 8, at 234.

153. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 66 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

154. *See* Tene & Polonetsky, *supra* note 59, at 320–22.

155. *See* CHITIKA, INC., 151 F.T.C. 494 (2011) (consent order and complaint for a case in which the FTC sued Chitika, Inc., a network advertiser engaging in behaviorally targeted advertising, for not respecting its privacy policy option for users to opt out of receiving tracking cookies).

156. *See* Kang, *supra* note 122.

157. *See supra* Part I.A.

158. FTC Act, 15 U.S.C. §§ 52–53.

CalOPPA does. Even if a user is unaware of the nature and extent of the collection and use of his or her personal information, the FTC cannot pursue a lawsuit if the company's practices are not unfair or deceptive. As long as a company abides by its privacy policy, it can usually avoid the FTC's purview.[159] The only other way the agency could reach a company's practices is for the conduct at issue to implicate COPPA (or the privacy provisions in Gramm-Leach-Bliley Act or HIPAA). The FTC simply cannot fill in all of the gaps left by the federal and state statutory scheme. Without a private cause of action, users must hope they fall under the FTC Act, COPPA, or CalOPPA (or a similar, applicable state law). These laws leave too many people without sufficient protection from the harms of companies' collection and dissemination of personal information.

III. A COMPREHENSIVE FEDERAL SOLUTION

This Part proposes a solution to the problems that the collection and dissemination of users' personal information present. A comprehensive federal statute is the ideal remedy to the issues raised in Parts I and II because it would best ensure uniform consumer protection. This proposal also takes the companies' and third parties' interests into account to create a balanced privacy scheme. A federal law is especially important at this time because of the risks that new technologies pose to user privacy, particularly those raised by increased mobile usage,[160] and the gaps in protection currently afforded to users. This Note's proposed federal online privacy statute, the Digital Privacy Act (DPA), will fill in the current gaps by ensuring that users are aware of what happens to their information and by providing remedies for privacy violations. The key elements of the DPA are an electronic signature requirement, clear and conspicuous privacy policies, and a private cause of action. This proposal also avoids rigidity and overly broad restrictions through FTC enforcement, which will preserve the flexibility necessary in a developing field. The DPA includes the below-described provisions.

---

159. *See* Ciocchetti, *supra* note 5, at 581. A recent Third Circuit opinion may have expanded the FTC's power to combat large-scale data breaches, however; *See* F.T.C. v. Wyndham Worldwide Corp., No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015). In 2008 and 2009, hackers obtained personal and financial information from 619,000 of Wyndham's consumers, resulting in $10.6 million in fraud loss. *Id.* at *2–3. The FTC alleged that Wyndham violated the FTC Act by failing to protect consumers' sensitive personal information. The Third Circuit, in dismissing Wyndham's motion to dismiss, held that the FTC has authority to regulate cybersecurity. *See id.* at *9.

160. *See supra* Part I.D.

A. Electronic Signature Requirement

As its foundation, the DPA would require companies with an online presence to mandate affirmative and consensual user acceptance to clear and conspicuous privacy policies. This requirement addresses the crux of the problems discussed in Part I.C: the lack of informed consent from users. User acceptance should take a form that facilitates conscious acquiescence, such as having the user input a virtual signature. One recent study on electronic signatures noted that participants viewed checking an "I Accept" box as less valid than a typed-in name or computer-generated signature.[161] The virtual signature component introduces a concrete contractual mentality to data collection and dissemination policy agreements; most companies' privacy policies currently only offer an "I Accept" option rather than an opportunity for the user to sign his or her name.

Although some users may still not devote the time to read the full terms and conditions, a person's signature can evoke feelings of acceptance of a contractual agreement, unlike clicking a button, which is seen as purely an obstacle to online activity.[162] As a practical matter, the requisite technology for users to digitally sign their name on computers and mobile devices, instead of typing it in or having the website or app generate it, is already available.[163] A signature implies intent to be bound by an agreement.[164] Electronic signatures also have federally recognized legal effect, which solidifies their legitimacy.[165] Both companies and users would most likely prefer that a user only be required to sign once, to ensure an efficient online experience for future uses. The DPA would not require a signature for each subsequent use in order to take advantage of the benefits of data collection and dissemination.[166] This may create problems for public devices, such as computers in a public library. The DPA would also require a company's agreement,

---

161. *See* Eileen Chou, *Paperless and Soulless: E-signatures Diminish the Signer's Presence and Decrease Acceptance*, 6(3) SOCIAL PSYCHOLOGICAL AND PERSONALITY SCIENCE 343, 346–47 (Dec. 2, 2014), http://spp.sagepub.com/content/early/2014/11/13/1948550614558841.full.pdf+html.

162. *See* Smithers, *supra* note 39.

163. *See, e.g.*, Jorge Rodriguez, *Signature: Sign Your Digital Documents*, APPSTORM (Sept. 15, 2011), http://mac.appstorm.net/general/document-signing-made-digital-with-signature/.

164. *See* 2 SAMUEL WILLISTON, WILLISTON ON CONTRACTS § 6:44 (4th ed. 1990).

165. *See* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7006 (2000). The statute defines "electronic signature" as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." *Id.* § 7006(5).

166. *See supra* Part I.B.

detailing its collection and dissemination practices, to let a user signify whether a device is private or public. If the device is public, a company would have to request a user's signature for any subsequent uses.

B. Clear and Conspicuous Privacy Policies

Clear and conspicuous privacy policies are a key requirement of the DPA because they are necessary for actual informed consent. Agreement to a privacy policy is essentially contractual; however, the user's acceptance of this implicit contract is called into question by online providers' practices. Valid acceptance of an offer requires knowledgeable consent, which is not present in many users' online agreements. As discussed above, companies often make users go to additional lengths to access their policies.[167] Further exacerbating the issue, policies are often needlessly complex and written in legalese.[168] The Commercial Privacy Bill of Rights Act of 2011 recognized this problem, calling for transparent company privacy policies.[169] Moreover, a recent study demonstrated that users, when informed of how often apps access and share their information, take affirmative steps to protect their privacy.[170] Taking this study into account, if online providers implement clear and conspicuous terms and conditions, then users will be able to make an informed decision about whether to agree to participate in them and what protective measures to take. Accordingly, the DPA would require users to agree to clear and conspicuous policies on collection and dissemination practices before site or app use.

A "clear" privacy policy should be written in plain English,[171] not complex legalese. "Conspicuous" means that the company's policy must be located where a user is reasonably likely to see it. Clear and conspicuous privacy policies should provide adequate notice for users to understand how companies will use their information. As an effective means of notifying users of the important parts of their privacy policies, the DPA would provide for a bullet-point summary in the same section where a user provides an electronic

167. *See* Ciocchetti, *supra* note 5, at 586.

168. *Id.* at 587–89.

169. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 201 (2011).

170. Byron Spice, *Study Shows People Act to Protect Privacy When Told How Often Phone Apps Share Personal Information*, CARNEGIE MELLON UNIVERSITY NEWS (Mar. 23, 2015), http://www.cmu.edu/news/stories/archives/2015/march/privacy-nudge.html.

171. *See* Ciocchetti, *supra* note 5, at 632.

signature, with a conspicuous link to the full policy. This summarized bullet-point privacy policy must, at a minimum, state the types of information the website collects, the uses that such information will be put to, specific third parties that will receive the information or that will directly collect information from the user, and, in general, the measures that the company takes to protect users' information. The bullet-point summary should be limited to one page, unless more space is necessary to provide the required information.

Such a concise, clear, and fully informative approach to conveying companies' privacy policies and precautionary strategies is critical given the recent increase in large-scale data breaches.[172] The DPA would not require that companies disclose specific data protection methods (i.e., it would not provide data breach perpetrators with a guide to circumventing a company's security). If companies must generally disclose to the public what protections they are providing, however, they may be incentivized to strengthen security measures. This type of motivation may help prevent incidents such as the IRS' data breach.[173] As Justice Sonia Sotomayor once remarked, "Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility."[174]

C. Private Cause of Action

The DPA would also create a private cause of action for users affected by a company's violations of the provisions. This component would reinforce the contractual nature of a user's acceptance of terms and conditions. Users do not currently view privacy policies as contracts; the DPA's electronic signature and clear and conspicuous policy requirements ideally would change that mindset. When two individuals contract with one another, one party may sue the other for breach. Since acceptance of a company's privacy policy is a form of contractual agreement, users should be able to sue for an online provider's breach of its terms and conditions. This would enable users to take matters into their own hands and pursue claims that the FTC may not be able to litigate. Without

172. *See supra* Part I.C.

173. *See supra* Introduction.

174. Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 35 (2d Cir. 2002).

this comprehensive statute, a user would depend on the FTC's authority under the FTC Act, COPPA, or a state privacy law such as CalOPPA. Despite the FTC's expertise in this area, it simply cannot catch each privacy policy violation.

A private cause of action would alleviate this problem by ensuring maximum privacy coverage for users.[175] Unlike the Commercial Privacy Bill of Rights Act of 2011, this provision would also give users leverage with the capacity to enter into class action lawsuits against companies that have violated the provisions of the statute.[176] The threat of a class action lawsuit, especially for online providers with vast numbers of users, will encourage compliance. This provision of the DPA shifts bargaining power to users. Currently, users must engage in a virtual Hobson's choice[177] between (1) accepting a policy and allowing their personal information to be mined, or (2) foregoing a useful, perhaps essential service. Although companies may oppose this element of the DPA, they would still retain sufficient leverage to incentivize user agreement to data collection and dissemination policies, as discussed below.

D. FTC Enforcement

The FTC has familiarity with issues related to the collection and dissemination of personal information, and should maintain an active role in the enforcement of the DPA. Accordingly, the DPA will confer primary enforcement power on the FTC to ensure that DPA privacy protections succeed. The agency will prove critical as both COPPA and the FTC Act have provided the agency with the requisite expertise, and the FTC has created the Division of Privacy and Identity Protection, which oversees consumer privacy, identity theft, and information security issues.[178] This division enforces COPPA and Section 5 of the FTC Act, which prohibits unfair or deceptive

---

175. *Cf.* Robert H. Lande & Joshua P. Davis, *Benefits from Private Antitrust Enforcement: An Analysis of Forty Cases*, 42 U.S.F. L. Rev. 879 (2008). While the FTC has enforcement power for antitrust violations, "[V]irtually the only way to secure redress for the victims of antitrust violations is through private litigation. . . . [P]rivate enforcement also plays a significant role in deterring antitrust violations." *Id.* at 883–84. The authors conclude that private enforcement complements governmental regulation of the industry. *Id.* at 905–07.

176. *See* Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. § 406 (2011).

177. *See* WEBSTER'S THIRD NEW INT'L DICTIONARY 1076 (1986) (defining a Hobson's choice as "an apparent freedom of choice where there is no real alternative").

178. *Division of Privacy and Identity Protection*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity (last visited Jan. 3, 2016).

acts or practices.[179] The FTC already has an existing framework for enforcing user privacy laws; it only lacks a specific federal mandate.

Notably, the DPA's private cause of action does not remove the FTC's ability to bring lawsuits against companies; individuals can still defer to the agency. Unlike individual parties, the FTC has the resources to investigate material violations of the statute. The agency has demonstrated its inclination and ability to successfully prevent companies' deceptive monitoring and tracking practices.[180] As would have been the case under the Do Not Track Me Online Act of 2011, the DPA would authorize the FTC to prescribe exact standards for online providers to follow.[181] This will allow optimal flexibility in applying the goals of the Act to new technologies.

E. Companies' Interests

Although users require more protection from the statutory scheme, companies' interests must also be taken into account. The collection and dissemination of users' personal information is a critical practice for businesses.[182] It also provides numerous benefits for users such as tailored advertising.[183] The DPA will not prevent companies from using behavioral advertising or people-based marketing or disseminating personal information. Companies will only have to adjust how their privacy policies are displayed and respect users' choices. This proposal does not strip companies of all bargaining power; they may still restrict the functionality of their services or even deny access if users do not agree to their data policies. If the service is valuable, consumers will most likely continue to use it and agree to the terms and conditions. Users already make similar valuations for paid-subscription services, so it will not place too high a burden on either side.

The DPA would also not incorporate the FTC's Do Not Track proposal, because it would restrict or eliminate the advantages of

---

179. *Id.*

180. *See* Press Release, Federal Trade Commission, Sears Settles FTC Charges Regarding Tracking Software (June 4, 2009), https://www.ftc.gov/news-events/press-releases/2009/06/sears-settles-ftc-charges-regarding-tracking-software (describing a settlement with Sears after the FTC alleged that Sears' software would "monitor consumers' online secure sessions–including sessions on third parties' Web sites–and collect information transmitted in those sessions, such as the contents of shopping carts, online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for web-based e-mails," in addition to tracking users' offline activity).

181. Do Not Track Me Online Act, H.R. 654, 112th Cong. § 3 (2011).

182. *See, e.g.*, Soma et al., *supra* note 33, at 12; Solove, *supra* note 37, at 970.

183. *See supra* Part I.B.

data collection and dissemination by preventing companies from tracking user activity and delivering a personalized online experience.[184] It might also force online providers to categorically deny access to their services to users who use the Do Not Track mechanism.[185] The sponsors of the Commercial Privacy Bill of Rights Act of 2011 also opted against a Do Not Track mechanism, feeling that such a function would result in the loss of industry support.[186] To ensure a compromise between users' and companies' interests, and to encourage online providers' compliance, the FTC's Do Not Track proposal would not be adopted. Do Not Track mechanisms can also be disregarded by websites, calling into question their effectiveness.[187]

In light of the intensified risks that mobile usage presents to consumers, it is important that Congress enact a comprehensive statutory scheme to ensure uniform protection. Current practices have proven insufficient to insulate users from the drawbacks of collection and dissemination of their personal information. The current system of FTC regulation and state privacy laws contains too many gaps in coverage. With the emergence of new technologies and unforeseen privacy consequences, Congress must establish a framework for consumer privacy protection that achieves a balance between the interests of users and companies. With a statutory foundation in place that creates an electronic signature requirement, a clear and conspicuous privacy policy requirement, and a private cause of action, which ensures a continued role for FTC regulatory power, Congress would both maximize benefits for companies and users and mitigate the disadvantages of collecting and disseminating users' personal information.

CONCLUSION

Advances in technology relating to the collection and dissemination of personal information have led to many benefits for both users and companies. Users take advantage of these practices to enjoy a personalized and efficient online experience. Companies use behavioral marketing and advertising, resulting in increased

184. Molly Jennings, *To Track or Not to Track: Recent Legislative Proposals to Protect Consumer Privacy*, 49 HARV. J. ON LEGIS. 193, 200 (2012).

185. *Id.*

186. *See* Kang, *supra* note 122.

187. *See* Cooper Quintin, *HealthCare.gov Sends Personal Data to Dozens of Tracking Websites*, ELECTRONIC FRONTIER FOUNDATION (Jan. 20, 2015), https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal-data.

sales and more efficient advertising strategies. Since aggregated personal information has actual economic value, companies also benefit from collecting and selling digital profiles of their customers. While these practices are entrenched in Web and mobile usage and facilitate modern lifestyles, they pose significant and tangible risks to users.

The current state of online privacy law does not provide users with sufficient security. Tort and contract law do not provide adequate remedies for users. There are simply too many gaps in the coverage of federal and state statutes and FTC regulation. Even if recently proposed statutes had been enacted, their solutions would not have completely solved the problems discussed in this Note. These failed proposals did not take both users' and companies' interests into account and would have still exposed individuals to the risks of data collection and dissemination. These proposed laws also did not fully address the issues presented by mobile usage.

This Note attempts to address the heart of the problem: users do not read privacy policies, rendering their knowledge and consent illusory. Aspects of contract law provide an informative context to solve this problem. Although it will be difficult to change user tendencies, the DPA's electronic signature, clear and conspicuous privacy policies, and private cause of action requirements will encourage informed decision-making in the context of Internet and app usage. If companies clearly state their data collection and dissemination practices and users are required to do more than just click "I Accept," users may gradually pay closer attention to the privacy risks. This would allow a user to make a fully informed choice, deciding whether the utility of the website or app is worth the mining of his or her personal data. The DPA would also maintain a balance in taking companies' interests into account. By excluding a Do Not Track requirement, the DPA preserves the advantages that companies derive from collecting and disseminating personal information. Its flexibility would allow companies to continue enjoying these benefits. The DPA fills in the statutory and regulatory gaps, while ensuring a balance between user and industry interests. With recent changes in technology and large-scale data breaches, it is essential that Congress provides a comprehensive statutory scheme as discussed in this Note.