Comparing Consent to Cookies: A Case for Protecting Non-Use

Meg Leta Jones & Jenny Lee†

Introduction

During Mark Zuckerberg's testimony before Congress in April 2018, eight different senators asked the Facebook CEO about European privacy rights and whether Americans should or would receive similar protections.[1] The European Union's General Data Protection Regulation (GDPR)[2] put European privacy squarely in front of American technology companies, users, and policymakers. Having long been criticized for a lackluster privacy regime, the United States (U.S.) is set to seriously consider broad national data protection legislation after California managed to pass the Consumer Privacy Act (CCPA),[3] which will go into effect in 2020 if not preempted by federal law.

Americans have always been aware of European privacy—which is quite varied among countries and cultures despite being newly unified under the GDPR—and vice-versa. This awareness has led to influence but not to harmonization until, perhaps, now that data resides and is processed in multiple locations around the world by complex corporate systems and entangled government agencies. The global nature of platforms like Facebook, and the pressure from a powerful regional governing

---

† Jenny Lee holds a Masters in Communication, Culture & Technology from Georgetown University and is a Ph.D. student at the Annenberg School for Communication at the University of Pennsylvania. Meg Leta Jones, J.D., Ph.D., is an Associate Professor of international technology policy at Georgetown University. The authors would like to thank the Cornell Law School community for their thoughtful feedback and engaging discussion on the topics included in this Article.

1. *Facebook, Social Media Privacy, and the Use and Abuse of Data*, U.S. Senate (Apr. 10, 2018), https://www.commerce.senate.gov/2018/4/facebook-social-media-privacy-and-the-use-and-abuse-of-data [https://perma.cc/TDB3-YXWG] [hereinafter Zuckerberg Hearing] (statement of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook).

2. Council Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) [hereinafter GDPR].

3. CAL. CIV. CODE § 1798.100 (West 2020).

body with the political will to dictate technical terms like the European Union (EU), present an opportunity for world-wide uniformity in settings.

Settings have long been central to privacy debates.[4] The oldest and most fundamental is opt-in versus opt-out for cookies.[5] Should data collectors have to obtain user consent by receiving some type of affirmative communication accepting these small bits of data on their computers? Or can one build a system that collects data and allows users to change the settings to meet their preferences?

The GDPR speaks directly to these settings by requiring affirmative consent, or opt-in, for those sites and services that choose to use consent as their legal basis (there are five other options) for collecting or processing data.[6] In November 2017, the Article 29 Working Party (A29WP) released guidelines on what consent meant within the GDPR.[7] The A29WP explained that consent only works as a lawful basis for processing "if a data subject is offered control and . . . a genuine choice with regard to accepting or declining the terms offered or declining them without detriment."[8] Consent must be freely given, meaning it cannot be part of non-negotiable terms and it cannot determine functionality of site or service.

The A29WP guidelines on consent also reminds controllers that consent in the GDPR is tied to consent under the draft ePrivacy Regulation, as most controllers are "likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software."[9] The EU is set to replace the ePrivacy Regulation with a new ePrivacy Regulation in the coming months, eliminating variation between member states.[10] Importantly, the new regulation covers more than traditional telecommunication operators like large established internet service providers, applying also to services like Gmail, Skype, Facebook Messenger, and WhatsApp.[11]

Very little scholarly or public attention has been paid to the ePrivacy Regulation, but a great number of lobbying groups have taken notice. Most recently, those lobbying efforts have resulted in the untimely death of Arti-

4. *See generally* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

5. David M. Kristol, *HTTP Cookies: Standards, Privacy, and Politics*, ACM TRANSACTIONS ON INTERNET HIST., Nov. 2001, at 151, 151.

6. GDPR, *supra* note 2, at art. 6(1)(a).

7. *See* Article 29 Data Prot. Working Party, *Guidelines on Consent Under Regulation 2016/679*, WP 259 (Nov. 28, 2017), *available at* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [https://perma.cc/WTZ8-4RCS] [hereinafter A29WP Guidelines].

8. *Id.* at 3.

9. *Id.* at 4.

10. *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 10 final (Oct. 1, 2017).

11. *See generally id.*

cle 10 of the ePrivacy Regulation, which dealt with privacy settings.[12]

Back in 2010, the Federal Trade Commission (FTC) began a "Do Not Track" (DNT) initiative that would allow users to effectively opt-out.[13] They tapped the World Wide Web Consortium (W3C), the organization that sets technical standards for the web, to work out the details through a multi-stakeholder working group. After years of back and forth, the W3C group finally came up with a recommendation in 2016, which has resulted in most browsers including a DNT setting that users can turn on today.[14] However, an October 2018 *Gizmodo* article titled *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, explained that very few sites actually respect the setting.[15]

This Article compares U.S. and EU responses to cookies, specifically detailing efforts to legally enforce user preferences and provide meaningful consent. Users have been trying to block cookies for as long as they have been aware of them.[16] The first *Wired* magazine article about cookies covered a program called PGPcookie.cutter that blocked cookies and could be downloaded for $29.95.[17] Remarkably, today, cookies, cookie banners, and click-throughs are *still* plaguing user experiences and web functionality. By analyzing W3C archives; stakeholder press releases and interviews; U.S. administrative documents; materials on the EU Cookie Directive; EU member state national cookie laws; and EU Commission, Parliament, and Council drafts, this Article will detail how each side of the Atlantic has attempted—and, so far, failed—to provide users with legally enforceable, consistent, and realistic consent to cookies.

Many privacy scholars and commentators in both the U.S. and the EU have commented on cookies and DNT as contemporary privacy issues. In the U.S., most privacy research at least touches on consent and often uses cookies as an example or an anecdote to represent some kind of online

12. IT-Pol, *EU Council Considers Undermining ePrivacy*, EUR. DIGITAL RIGHTS (July 25, 2018), https://edri.org/eu-council-considers-undermining-eprivacy/ [https://perma.cc/UV3X-RLCG].

13. F.T.C., PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 4–5 (2012) [hereinafter FTC Report].

14. Nick Doty et al., *Tracking Compliance and Scope*, W3C (Apr. 26, 2016), https://www.w3.org/TR/2016/CR-tracking-compliance-20160426/ [https://perma.cc/8W6S-PQ6A].

15. Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, GIZMODO (Oct. 15, 2018, 10:56 AM), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324 [https://perma.cc/866A-HU62].

16. A *Financial Times* article by future technology venture capitalist Tim Jackson, raised privacy concerns about cookies for the first time in February of 1996. He wrote,

> [m]ost extraordinary of all, this information can be stored on customers' own PCs without their knowledge. It can be kept in a form so that only the company that collected the information can benefit from it . . . . Moreover [sic] there appears to be only one way to disable the facility: by manually amending or deleting the COOKIE.TXT file containing all the cookies.

Tim Jackson, *This Bug in Your PC is a Smart Cookie*, FIN. TIMES, Feb. 12, 1996, at 15.

17. James Glave, *PGP Lets You Take Charge of Your Cookies*, WIRED (Dec. 10, 1996, 8:00 PM), https://www.wired.com/1996/12/pgp-lets-you-take-charge-of-your-cookies/ [https://perma.cc/ZWQ7-ZYE8].

tracking or privacy issue.[18] Some have focused more narrowly on cookies and others on DNT.[19] Broad academic research on DNT boomed in the early-to-mid 2010s, when the proposal was adopted by the FTC, and implementation debates ensued. The research touched on DNT from several different angles. Some, like Ceren Budak, Sharad Goel, Justin Rao, and Georgios Zervas, tackled the topic of DNT's economics, finding that most of the top 10,000 content providers could generate comparable revenue by charging site visitors $2 per month if DNT were strictly implemented.[20] Others, like Alicia Shelton, took note of the difficulties in enacting federal privacy legislation and, instead, argued for the implementation of DNT at the state level because state lawmakers are in a better position to efficiently "enact[ ] legislation . . . in [this] rapidly advancing field."[21]

Many researchers such as Angelica Nizio, Matthew Kirsch, and Stephanie Kuhlmann have detailed the ongoing discussions of DNT, ultimately arguing that the proposals of implementation were full of logistical issues to be solved by legislative enforcement.[22] Molly Jennings analyzed the two legislative proposals of cookie privacy at the time: The Commercial Privacy Bill of Rights and the Do-Not-Track Online Act (DNTOA), favoring the former for its flexibility to evolve along with technology.[23] Some others, such as Aleecia McDonald, Jon Peha,[24] Chris Hoofnagel, Jennifer Urban, and Su

18. *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 148 (Yale Univ. Press, 2012); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 54 (Harvard Univ. Press 2018); VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 153–56 (John Murray 2013); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 157 (Stanford Univ. Press 2010); NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 164 (Oxford Univ. Press 1st ed. 2015); DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 24–26 (N.Y. Univ. Press 2004).

19. *See generally* Lynette I. Millett et al., *Cookies and Web Browser Design: Toward Realizing Informed Consent Online*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 46 (ACM 2001).

20. Ceren Budak et al., *Understanding Emerging Threats to Online Advertising*, *in* PROCEEDINGS OF THE 2016 ACM CONFERENCE ON ECONOMICS AND COMPUTATION 561, 575 (ACM 2016).

21. Alicia Shelton, *A Reasonable Expectation of Privacy Online: "Do Not Track" Legislation*, 45 U. BALT. L.F. 35, 49 (2014).

22. *See generally, e.g.*, Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, 18 RICH. J.L. TECH. 2 (2011); 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 (2011); Angelica Nizio, *Taking Matters into Its Own Hands: Why Congress Should Pass Legislation to Allow the FTC to Regulate Consumer Online Privacy with a "Do Not Track" Mechanism*, 2014 U. ILL. J.L., TECH. & POL'Y 283 (2014).

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

24. Aleecia M. McDonald & Jon M. Peha, *Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature*, TELECOMM. POL'Y RES. CONF. 1, 1 (2011).

Li,[25] followed suit, revealing the gap between user recognition and expectation of DNT along with the realities of the implementation proposals. Joshua Fairfield elaborated on this argument, contending that consumers would not benefit from DNT if the onus of research and use fell onto them.[26] Meanwhile, Galina Fomenkova argued for more choices and decisions for users.[27] Additionally, Omer Tene and Jules Polonetsky proposed that the underlying issue behind all of the problems with DNT implementation was that no conversation had been had about which kinds of consumer tracking are socially acceptable and which are "unnecessar[ily] evil."[28] Recently, McDonald updated the privacy community on DNT, detailing the reasons for why the technology was never implemented and how that will likely change.[29]

In the EU, scholars such as Eleni Kosta[30] and Frederik Zuiderveen Borgesius[31] have focused on cookies as they relate to the EU's pair of Directives, which are discussed below. Few have compared the way in which the U.S. approaches consent with the European approach.[32] Privacy scholarship has a short history, but it is steep in comparison. Samuel Warren and Louis Brandeis were inspired by European legal concepts of privacy and personhood.[33] Willis Ware and his committee at the Department of Health, Education, and Welfare reference numerous European countries in their famous 1973 report, *Records, Computers, and the Rights of Citizens*.[34] Also, David Flaherty's groundbreaking *Protecting Privacy in Surveillance Societies*[35] and Colin Bennett's *Regulating Privacy*[36] richly and systemati-

25. Chris Jay Hoofnagle et al., *Privacy and Modern Advertising: Most US Internet Users Want "Do Not Track" to Stop Collection of Data About Their Online Activities*, Amsterdam Privacy Conf. 1, 1–2 (2012).

26. Joshua A. T. Fairfield, *Do-Not-Track as Default*, 11 Nw. J. Tech. & Intell. Prop., 576, 578 (2013).

27. Galina I. Fomenkova, *For Your Eyes Only? A 'Do Not Track' Proposal*, 21 Info & Comm. Tech. L. 33, 41 (2012).

28. 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, 284 (2012).

29. *See generally* Aleecia M. McDonald, *Stakeholders and High Stakes: Divergent Standards for Do Not Track*, *in* The Cambridge Handbook of Consumer Privacy 251 (Jules Polonetsky et al. eds., Cambridge Univ. Press 2018).

30. Eleni Kosta, *Peeking into the Cookie Jar: The European Approach Towards the Regulation of Cookies*, 21 Int'l J.L. & Info. Tech. 380, 381-90 (2013).

31. *See generally* Frederik Zuiderveen Borgesius, *Behavioral Targeting, a European Legal Perspective*, IEEE Security & Privacy, Jan.–Feb. 2013, at 82.

32. *See generally* McDonald & Peha, *supra* note 24.

33. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

34. U.S. Dep't of Health, Educ. & Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems 168–74 (1973).

35. *See generally* David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, & the United States (Univ. of N.C. Press 1989).

36. *See generally* Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell Univ. Press 1992).

cally compared Western countries' approaches to data rights and obligations.

For all their differences, the U.S. and the EU have both failed to legally enforce a DNT signal. Comparing the ways in which the two regions treat cookies and browser defaults reinforces this distinction. Revisiting cookies and DNT, however, also requires an investigation into the power, platforms, and political constructions of the user. What exactly does a DNT signal protect and what should it enforce? Instead of focusing on the user and her choice predicament, we utilize Sally Wyatt's "non-user"[37] to consider how DNT may more appropriately be understood to protect resistance and non-use.

The Article takes a comparative approach to understanding cookies and DNT, both as a historical legacy system of the web and as a contemporary privacy issue. It tells an intertwined set of stories beginning in the mid-1990s and ending with legislative proposals currently being considered in each region, such as the federal data protection legislation in the U.S. and the ePrivacy Regulation in the EU. Over that same period, we point to the evolution of sites to platforms and identify an overlooked type of political data participation: non-use. We argue that, in fact, DNT presents a unique opportunity for international interoperability and should be reconsidered and legally enforced in two different ways, which protect the digital privacy of their respective regions.

I. U.S. History of "Do Not Track"

In 1989, the World Wide Web (the Web) was proposed and sketched up by a young British engineer, Tim Berners-Lee, while he was working at the *Conseil Européen pour la Recherche Nucléaire* (CERN) in Geneva, Switzerland.[38] By the end of 1990, Berners-Lee had produced the first webpage, which was built on elements he had also managed to write over that year: HTML, HTTP, URL (then URI), and the first web browser (WorldWideWeb.app)—all of which were intentionally and explicitly non-proprietary.[39] In 2018, during an interview, Berners-Lee reflected on his project, which was later further ushered into society by him and W3C—both housed at the Massachusetts Institute of Technology (MIT). He stated that he was "devastated" by what the Web had become.[40] He explained, "[t]he spirit there was very decentralized. The individual was incredibly

37. *See* Sally Wyatt, *Non-Users Also Matter: The Construction of Users and Non-Users of the Internet*, *in* How Users Matter: The Co-Construction of Users and Technology 67, 72–75 (Nelly Oudshoorn & Trevor Pinch eds., MIT Press 2003).

38. *History of the Web*, World Wide Web Found., https://webfoundation.org/about/vision/history-of-the-web/ [https://perma.cc/AJD8-KPWT] [hereinafter World Wide Web Found.]; *About CERN*, CERN, https://home.cern/about [https://perma.cc/VNF8-CP5K].

39. World Wide Web Found., *supra* note 38.

40. Katrina Brooker, *"I Was Devastated": Tim Berners-Lee, the Man Who Created the World Wide Web, Has Some Regrets*, Vanity Fair (July 1, 2018), https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets [https://perma.cc/VA78-XTLZ].

empowered. It was all based on there being no central authority that you had to go to to [sic] ask permission . . . . That feeling of individual control, that empowerment, is something we've lost."[41] That spirit had been embodied by those working in the U.S. to bring the Web to the masses,[42] but so had the entrepreneurial spirit of Silicon Valley.[43]

In 1994, just over a year after CERN announced to the public domain its release of the software required to run a web server, a basic browser, and a code library,[44] Lou Montulli created a shopping cart for the product's team at Netscape.[45] He came up with the "persistent client state object," better known today as the cookie.[46] The cookie sparked conversation about creating or maintaining statefulness among developers who were also considering intellectual property tracking and tag propagation.[47] Throughout 1995, online discussion boards explored the pros, cons, and standardization of methods for creating statefulness.[48] At the time, Netscape controlled over 80% of the browser market, holding significant power to shape a budding digital culture.[49] Today, the cookie default built into Netscape Navigator, and Montulli's decision to allow third-party cookies, have become the infrastructure that supports contemporary platforms.[50]

Cookies were not covered by the media beyond more than a passing reference until a 1996 *Financial Times* article suggested that they may pose a privacy threat.[51] As soon as cookies were brought to the public's attention, tools were created to block them. For instance, the first article in *Wired* from December 1996 covered a tool to combat cookies called PGPcookie.cutter—as well as later versions of both, Microsoft's Internet

41. *Id.*

42. FRED TURNER, FROM COUNTERCULTURE TO CYBERCULTURE: STEWART BRAND, THE WHOLE EARTH NETWORK, AND THE RISE OF DIGITAL UTOPIANISM 135 (Univ. Chi. Press 2006).

43. *Id.* at 149–51.

44. Marina Giampietro, *Twenty Years of a Free, Open Web*, CERN (Apr. 30, 2013), https://home.cern/news/news/computing/twenty-years-free-open-web [https://perma.cc/8JDC-FM9T].

45. John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. TIMES (Sept. 4, 2001), https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html [https://perma.cc/MRU4-SDQQ].

46. *Id. See also* Lou Montulli, *The Reasoning Behind Web Cookies*, IRREGULAR MUSINGS OF LOU MONTULLI (May 14, 2013), https://montulli.blogspot.com/2013/05/the-reasoning-behind-web-cookies.html [https://perma.cc/8Z6T-LA2E].

47. Brian Thomas, *Recipe for E-Commerce*, IEEE INTERNET COMPUTING Nov.–Dec. 1997, at 72, 73.

48. *See, e.g.*, E-mail from Shel Kaphan, Vice President of Research & Dev. and Chief Tech. Officer, Amazon, to Dave Ladd, World Wide Web Consortium (Dec. 1, 1995, 1:39 PM), *available at* https://lists.w3.org/Archives/Public/www-talk/1995NovDec/0202.html [https://perma.cc/2SRB-9YDQ].

49. Jay Hoffmann, *The History of the Browser Wars: When Netscape Met Microsoft*, HIST. WEB (June 19, 2017), https://thehistoryoftheweb.com/browser-wars/ [https://perma.cc/9FYM-VR8B].

50. Montulli, *supra* note 46.

51. Jay P. Kesan & Rajiv C. Shah, *Deconstructing Code*, YALE J.L. & TECH., 277, 300 (2003–2004). *See generally* Jackson, *supra* note 16.

Explorer and Netscape's Navigator—which allowed users to block or delete cookies.[52] These tools would be referred to as Privacy Enhancing Technologies (PETs),[53] which were seeds for what is now an entire field of privacy and usable security engineering. Some of the first high profile efforts at PETs were attempts to empower the user by better and more efficiently understanding privacy policies, including grades, labels, and certifications.[54] Another set of projects include tools to block or control cookies as well as other trackers and advertisings, like browser extension apps and dashboards.

Policymakers were also prompted to address cookies. The U.S. Department of Energy's Computer Incident Advisory Capability issued an information bulletin in 1998, wherein annoyed authors explained:

> The vulnerability of systems to damage or snooping by using web browser cookies is essentially nonexistent. Cookies can only tell a web server if you have been there before and can pass short bits of information (such as a user number) from the web server back to itself the next time you visit . . . . Information about where you come from and what web pages you visit already exists in a web server's log files and could also be used to track users browsing habits, cookies just make it easier.[55]

Their solution was: "No files are destroyed or compromised by cookies, but if you are concerned about being identified or about having your web browsing traced through the use of a cookie, set your browser to not accept cookies or use one of the new cookie blocking packages."[56]

Similarly, the FTC issued *Privacy Online: A Report to Congress* (the Report) in 1998, explaining what cookies are and the need for privacy protections to encourage those who are still hesitant to come online. In considering consent, the Report explains:

> In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.[57]

Not everyone saw cookies as harmless, however. In January 2000, a class action complaint was filed against DoubleClick, Inc.[58]—the online

52. Glave, *supra* note 17.

53. Lydia F. de la Torre, *What Are Privacy-Enhancing Technologies (PETs)?*, MEDIUM (Mar.7, 2019), https://medium.com/golden-data/what-are-privacy-enhancing-technologies-pets-8af6aea9923 [https://perma.cc/8TKM-LZRF].

54. *See* Joel R. Reidenberg et al., *Trustworthy Privacy Indicators: Grades, Labels, Certifications and Dashboards*, 96 WASH. U. L. REV. 1409, 1413 (2019).

55. *Internet Cookies*, U.S. DEP'T ENERGY: CIAC (Mar. 12, 1998, 11:00 PM), https://web.archive.org/web/20090117080854/http://www.ciac.org/ciac/bulletins/i-034.shtml [https://perma.cc/6LR4-ZXYT].

56. *Id.*

57. F.T.C., PRIVACY ONLINE: A REPORT TO CONGRESS 9 (1998).

58. In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001).

advertising giant that used third-party cookies to track users and deliver ads for its 11,000 affiliates (at the time)[59]—by its users, claiming that the companies used cookies to collect information users would not expect to be collected and did so without users' knowledge, and that this collection was in violation of the Stored Communications Act;[60] the Wiretap Act;[61] and the Computer Fraud and Abuse Act (CFAA);[62] as well as New York State's common law crimes of invasion of privacy,[63] trespass to property,[64] unjust enrichment, and consumer deception and unfair business practices.[65] In finding for DoubleClick across the board, the court noted that plaintiffs could not meet the minimum damages requirement of $5,000 under the CFAA because it assessed damage each time a cookie was accessed individually and explained that affirmative steps to prevent wrongful access were free.[66] For example, users could simply download an "opt-out cookie" from DoubleClick's website.

Since the early 2000s, major online advertisers have also offered users the choice to opt-out of cookie-based tracking.[67] Though enabled by default, cookies could be turned off by visiting an advertising network's website and manually de-selecting the option.[68] While this option was a step in the right direction, opt-out cookies also came with numerous flaws. First, users bore the brunt of the work, tasked with searching and changing selections for ad networks one by one. Second, their opt-out choices were too easily made impermanent. If a user, in an attempt to further protect their information, deleted their browser cookies, they would lose their opt-out cookies as well. Users would be forced to repeat the time-consuming process each and every time.

In late October of 2007, a coalition of U.S. privacy groups, led by the World Privacy Forum, proposed their own PET to protect users from unwanted online behavioral tracking.[69] In the wake of controversial acquisitions of advertising technology companies such as Microsoft's acquisition of aQuantive and Google's acquisition of DoubleClick, the proposal came at a time of increasing user surveillance. Evoking the success and name recognition of the "Do Not Call" list, these groups called their proposal "Do Not Track."[70] DNT would require online advertising networks to register

59. *Id.*
60. 18 U.S.C. § 2701.
61. 18 U.S.C. § 2511.
62. 18 U.S.C. § 1030.
63. N.Y. CIV. RIGHTS LAW §§ 50–51 (Consol. 2019).
64. N.Y. PENAL LAW § 140.05 (Consol. 2019).
65. N.Y. GEN. BUS. LAW § 349 (Consol. 2012).
66. In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 520 (S.D.N.Y. 2001).
67. *See, e.g.*, *Interest-Based Advertising and Opting Out*, OPENX, https://www.openx.com/legal/interest-based-advertising/ [https://perma.cc/B9DM-RZ7C].
68. *Id.*
69. Ari Schwartz et al., *Consumer Rights and Protections in the Behavioral Advertising Sector*, WORLD PRIVACY F. 1, 4 (2007), https://www.worldprivacyforum.org/wp-content/uploads/2008/04/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf [https://perma.cc/Z2VB-8587].
70. *Id.*

their cookie-placing domains (as well as the domains of other user-tracking technologies) with the FTC, where they would be compiled into a machine readable list.[71] These networks were responsible for keeping the list up-to-date while the FTC ensured that the list would be easily found on its website. From there, browsers and users alike could download the DNT list and effectively block tracking with ease. But the idea quickly lost momentum and was largely forgotten until 2010.

However, one issue addressed by DNT, the issue of opt-out cookie impermanence, was tackled by Google. Shortly after the completion of its DoubleClick acquisition, Google released a browser add-on called "Keep My Opt-Outs" that allowed users to delete cookies and maintain their opt-out choices.[72] While the program was an improvement on the existing approach, "Keep My Opt-Outs" only applied to DoubleClick—one advertising network out of hundreds.

Soon after Google's add-on was released, privacy researcher Christopher Soghoian modified "Keep My Opt-Outs" to include several other advertising networks. Naming his tool "Targeted Advertising Cookie Opt-Out," or TACO for short, Soghoian published the add-on and received hundreds of downloads.[73] Due to the burden of updating a growing list of ad networks, Soghoian teamed up with Mozilla's Sid Stamm to shift tactics and turn to a browser header approach.[74] This new add-on included two browser headers for all HTTP requests, establishing a clear sign of user intent for both behavioral tracking *and* general tracking.[75] If honored, the headers would repair the loophole that ad networks had long relied on. Thus, even after users opted out of cookie-based tracking, advertisers could continue to track users, they just could not customize user ads. Soghoian's and Stamm's new-and-improved tool was a holistic defense, but it relied completely on advertising networks to honor the requests.

Though the headers approach found little support among advertising networks, the general tracking header (X-Do-Not-Track: 1) found an audience with the privacy community and with the FTC. Chairman Jon Leibowitz showed support for the DNT header during his Senate testimony in March 2011,[76] and Commissioner Julie Brill followed suit when speaking at a privacy conference a few months later.[77] The FTC's support was fur-

71. *Id.*

72. Sean Harvey & Rajas Moonka, *Keep Your Opt-Outs*, GOOGLE PUB. POL'Y BLOG (Jan. 24, 2011), https://publicpolicy.googleblog.com/2011/01/keep-your-opt-outs.html [https://perma.cc/644H-US38].

73. Christopher Soghoian, *The History of the Do Not Track Header*, SLIGHT PARANOIA (Jan. 21, 2011), http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html [https://perma.cc/Y8K9-GCCJ].

74. *Id.*

75. *Id.*

76. *The State of Online Consumer Privacy,* FTC 1, 6–9, 12–17 (2011), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-state-online-consumer-privacy/110316consumerprivacysenate.pdf [https://perma.cc/F2X4-C67P].

77. Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at the Proskauer on Privacy Conference (Oct. 19, 2010) (transcript available at http://

ther entrenched with the publication of their preliminary staff report, which contained a formal endorsement of the tool.[78] DNT was back in the headlines, more than three years after its first interactions were proposed.[79]

If DNT suffered from issues of non-exposure in the past, it faced no fewer challenges with the new influx of attention. Disagreements abounded around the definitions and implementations of DNT, with browsers launching their own interpretations of the technology while policy makers, privacy scholars, and advertising executives struggled to determine a universal standard. From the start, DNT's fate rested in the hands of a hundred different members in the W3C Tracking Protection Working Group (the Working Group). Finding a consensus proved impossible. By September 2013, the Digital Advertising Alliance (DAA), an enormous force that represents hundreds of advertising groups like the Association of National Advertisers and the American Advertising Federation, departed, citing irreconcilable differences.[80] Pointing to the fact that two years had gone by without a definition of "tracking" created, the DAA declared that the group had "reached the end of its useful life."[81]

Meanwhile, several browsers launched their own interpretations of user choice with regard to tracking. Google elected to go the opt-out route, expanding on the DAA's self-regulatory principles with its "Keep My Opt-Outs" approach.[82] Mozilla, on the other hand, maintained that browser headers were better for users.[83] It argued that headers removed the burden of setting individual opt-out cookies for hundreds of companies.[84] The HTTP headers also carried the benefit of preemption, establishing user consent before setting or sending any cookies.[85] But the header itself was not enough; whether or not companies would honor the request was still in question. Microsoft chose to approach DNT the way it had first been proposed—in list form. Internet Explorer 9 came with an opt-in mechanism that allowed users to create, publish, and apply "Tracking Protection Lists."[86] Domains placed on the list would only be visited by the browser if the user clicked on a direct link or typed in the direct website address. In

---

www.ftc.gov/speeches/brill/101019proskauerspeech.pdf [https://perma.cc/GN93-FBUC]).

78. *See generally* FTC Report, *supra* note 13.

79. *See generally, e.g.*, Edward Wyatt & Tanzina Vega, *F.T.C. Backs Plan to Honor Privacy of Online Users*, N.Y. TIMES (Dec. 1, 2010), https://www.nytimes.com/2010/12/02/business/media/02privacy.html [https://perma.cc/UQN9-NHNL].

80. E-mail from Lou Mastria, Dig. Advert. All., to Jaffe Jeff, World Wide Web Consortium (Sept. 17, 2013, 05:17 AM), *available at* https://lists.w3.org/Archives/Public/public-tracking/2013Sep/0061.html [https://perma.cc/YXY5-CE5F].

81. *Id.*

82. Harvey & Moonka, *supra* note 72.

83. Alex Fowler, *Advertisers and Publishers Adopt and Implement Do Not Track*, MOZILLA BLOG (Mar. 30, 2011), https://blog.mozilla.org/blog/2011/03/30/advertisers-and-publishers-adopt-and-implement-do-not-track/ [https://perma.cc/C9C7-ZS3U].

84. *Id.*

85. *Id.*

86. *IE9 and Privacy: Introducing Tracking Protection*, MICROSOFT (Dec. 6, 2010), https://blogs.msdn.microsoft.com/ie/2010/12/07/ie9-and-privacy-introducing-tracking-protection/ [https://perma.cc/527H-PXHP].

2012, however, Microsoft announced that Internet Explorer 10 would have DNT turned on by default for every user.[87] Though this proposal was met with a quick death, it represented another divergent voice in the DNT-implementation debate.[88]

Meanwhile, an equally contentious and conflicting debate was occurring in the legislative branch, where several online behavioral tracking bills were introduced. In early 2011, California's Senator Alan Lowenthal proposed drafting state-wide regulations for DNT with Senate Bill 761.[89] Nearly three years later, the State passed Assembly Bill 370,[90] a transparency law that merely required California-based companies to alert users of how they respond to DNT requests.

The federal level experienced even less success with regulating DNT. Representatives Jackie Speier, Alcee Hastings, and Bob Filner proposed the Do Not Track Me Online Act (DNTMOA) in February of 2011.[91] It would have empowered the FTC to establish standards for an online opt-out mechanism that would allow users to prohibit collection of covered information. Covered entities would be required to respect the choice of a user's tracking settings. Two months later, Senators John Kerry and John McCain proposed their Commercial Privacy Bill of Rights Act (CPBR), an alternative approach to regulating tracking settings.[92] Unlike DNTMOA, the Kerry-McCain bill took a wider stance and laid out a broad privacy framework. Users would gain opt-out settings for the unauthorized use of their personal information but would also find privacy protection through transparency and increased data security mechanisms. The very next day, Representatives Cliff Stearns and Jim Matheson introduced the Consumer Privacy Protection Act (CPPA) to allow users the choice to preclude the sale or disclosure of personal information for purposes other than a transaction with the user for up to five years.[93] The Do-Not-Track Online Act of 2011 (DNTOA) came afterward, its provisions closely resembling those of DNTMOA.[94] The Do Not Track Kids Act of 2011 (DNTKA) focused specifically on user control of the online behavioral tracking of children, barring all ads targeted to them.[95] And in early 2012, President Barack Obama

87. *Advancing Consumer Trust and Privacy: Internet Explorer in Windows 8*, MICROSOFT (May 31, 2012), https://blogs.microsoft.com/on-the-issues/2012/05/31/advancing-consumer-trust-and-privacy-internet-explorer-in-windows-8/ [https://perma.cc/K8SV-TXN3].

88. *E.g.*, *An Update on Microsoft's Approach to Do Not Track*, MICROSOFT (Apr. 3, 2015), https://blogs.microsoft.com/on-the-issues/2015/04/03/an-update-on-microsofts-approach-to-do-not-track/ [https://perma.cc/N2CN-AWL4].

89. S. 761, 112th Cong. (2011) (as amended by Senate, Mar. 24, 2011).

90. Assemb. B. 370, 2013 Assemb., Reg. Sess. (Cal. 2013).

91. Do Not Track Me Online Act, H.R. 654, 112th Cong. (1st Sess. 2011).

92. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (1st Sess. 2011).

93. Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (1st Sess. 2011).

94. Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (1st Sess. 2011) [hereinafter DNTOA].

95. Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (1st Sess. 2011).

introduced the White House's proposal for a Consumer Privacy Bill of Rights.[96] Though the proposal included a section on individual user control, the details on how companies might provide users with opt-in or opt-out privileges were sparse.[97] None of these bills ever became law.

Privacy scholars and researchers hotly debated the effectiveness of these bills, coming to an overwhelming agreement that none were enough to tackle the multi-faceted issues of user privacy. The DNTMOA and DNTOA were criticized, for example, for their "vague terminolog[ies]," which left gaping holes in the protections of user tracking, while also shutting down first-party uses of data.[98] Comparisons were also made between CPBR and DNTOA. The former would require companies to adhere to specific security practices when collecting user data and give users the right to access, correct, and control their own data.[99] It also required that users opt in to the collection of personal information, as well as limited data collection to the minimum amount required for the transaction's completion. It did not, however, include a DNT mechanism.[100] DNTOA, on the other hand, required a mandatory, browser-based DNT tool that would allow users to opt out of behavioral tracking. Some researchers argued that the focus on DNT as a panacea for user privacy issues was misguided. DNTOA offered a solution to a very specific privacy problem—online behavioral tracking—but its implementation would fall short of broadly protecting users.[101] CPBR, despite not including a DNT mechanism, was argued to be a "more comprehensive piece of [privacy] legislation" that insisted on privacy by design and data minimization, and thus would "fit better with the existing Internet architecture."[102]

Beyond the details of the bills' provisions, many found fault with the foundations of the proposed legislation—namely, the procedures for user consent and control. They argued that bills like DNTOA and DNTMOA, which required users to research, understand, and set settings by hand, were inherently at odds with the concept of true consent because they considered silence (in the form of an uneducated or unaware user) to represent a user's active decision to be tracked.[103] Others pointed out that these bills were mere band-aids on the issue of privacy rights. To them, the arguments between companies and legislators over the specifics of DNT disguised the true question at hand: what issues of data privacy are socially acceptable, and which are "unnecessary evil[s]"?[104] Until greater discussions on effi-

96. *See generally* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012) [hereinafter CPBR].

97. *Id.*

98. *E.g.*, 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, 269 (2011).

99. CPBR, *supra* note 96, at 1.

100. *Id.* at 12–13.

101. DNTOA, *supra* note 94.

102. Jennings, *supra* note 23, at 199.

103. Fairfield, *supra* note 26, at 579.

104. Tene & Polonetsky, *supra* note 28, at 284.

ciency versus privacy, law enforcement versus individual rights, and reputation versus freedom of speech, were had, these bills could not properly address the issues at hand.

Despite all the differing opinions and interpretations from the legislative, academic, and technical sides, the Working Group and DNT both survived for several more years. These years were full of ups and downs, with several resignations within the Working Group and a widespread retraction of adherence to DNT by major browsers like Yahoo.[105] In 2015, after many years of back-and-forth, the Working Group announced that their two specifications, Tracking Preference Expression (TPE) and Tracking Compliance and Scope (TCS), had progressed to Candidate Recommendation and Last Call, respectively.[106] But that success fell at the final hurdle and failed to lead to the creation of a universal standard. As of January 2019, the Working Group was closed and both TPE and TCS retired, the W3C cited reasons of insufficient deployment of DNT extensions and support from the industry.[107]

Even still, DNT shows signs of life, particularly in the American public's renewed interest after the Cambridge Analytica scandal.[108] Though much of the outrage associated with Cambridge Analytica centered on the electoral effects of the Russian-paid advertisements, many others understood that the root of the issue lies with consent.[109] During Zuckerberg's testimony in front of the Senate Judiciary and the Senate Committee on Commerce, Science, and Transportation, a few senators pressed the executive on violations of privacy. Senator Dick Durbin presented a series of hypothetical scenarios—"would Mr. Zuckerberg like to tell the world the name of the hotel in which he is staying? What about the names of the people he has messaged in the past week?"—to make his greater point on user expectations of privacy. In what was one of the testimony's most salient moments, Senator Durbin pushed Zuckerberg on "what information Facebook is collecting on [users], who Facebook is sending the information to, and whether Facebook asked the user in advance for permission to do that."[110]

Senator Richard Blumenthal brought up Facebook's 2011 consent

105. Ginny Marvin, *Yahoo Ditches "Do Not Track": Lack of Standards Too Confusing*, MARKETING LAND (May 1, 2014, 3:00 PM), https://marketingland.com/yahoo-ditches-track-will-signal-end-privacy-initiative-82384 [[https://perma.cc/42JP-ZQ6F].

106. Posting of Justin Brookman, justin@jbrookman.com, to public-tracking@w3.org (July 6, 2015, 7:17 PM), *available at* https://lists.w3.org/Archives/Public/public-tracking/2015Jul/0000.html [https://perma.cc/WHY6-N5R4].

107. Posting of Xueyuan Jia, xueyuan@w3.org, to w3c-ac-members@w3.org (Jan. 17, 2019, 8:27 PM), *available at* https://lists.w3.org/Archives/Public/public-tracking/2019Jan/0000.html [https://perma.cc/4A2C-V6DV].

108. Andrew Perrin, *Americans Are Changing Their Relationship with Facebook*, PEW RES. CTR. (Sept. 5, 2018), https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/ [https://perma.cc/3END-3TN2].

109. *See generally* Jim Isaak & Mina J. Hanna, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, COMPUTER, Aug. 2018, at 56 (2018).

110. Zuckerberg Hearing, *supra* note 1.

decree with the FTC,[111] which required that the platform receive user consent before making any changes to their privacy settings. Referencing thisisyourdigitallife's ability to gather not only the individual user's personal information, but the personal information of all of their friends without their knowledge, he asked: "Doesn't [thisisyourdigitallife's] terms of service conflict with the FTC order?"[112]

Following the testimony, Senators Blumenthal and Ed Markey introduced the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act.[113] The bill established privacy protection for customers of online edge providers,[114] offering an opt-in requirement that shifted the burden of consent off of users and onto platforms like Facebook. A few weeks later, Senators Amy Klobuchar and John Kennedy introduced their bipartisan Social Media Privacy and Consumer Rights Act.[115] The bill would maintain current opt-out capabilities for users but would demand plain language transparency from companies about data usage and behavioral tracking. In December 2018, Senator Brian Schatz , along with fourteen other senators, introduced the Data Care Act of 2018.[116] Using the terms "care, loyalty, and confidentiality" to describe the data protection duties that online service providers must adhere to, the bill evoked values already prescribed to those in other industries, such as healthcare.[117]

Other recent privacy legislation drafts include the Center for Democracy & Technology's bill,[118] which touches on tracking and consent in a section devoted to the most sensitive data types, such as biometric information and health information.[119] Intel threw its own hat into the ring with a more company-friendly proposal that includes a safe harbor provision to protect companies from civil action.[120] Organizations and institu-

111. *See* Emily Stewart, *Senators on Facebook's Potential $5 Billion Fine: Not Good Enough*, VOX (May 7, 2019, 2:50 PM), https://www.vox.com/recode/2019/5/7/18535631/facebook-ftc-fine-richard-blumenthal-josh-hawley [https://perma.cc/2T8A-J8JM]. *See also* Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011) (available at http://ftc.gov/opa/2011/11/privacysettlement.shtm [https://perma.cc/H3ZV-43CN]).

112. Zuckerberg Hearing, *supra* note 1.

113. *See generally* Customer Online Notification for Stopping Edge-provider Network Transgressions, S. 2639, 115th Cong. (2d Sess. 2018).

114. Edge providers are websites and applications that use the customer's internet service provider to deliver content. The term "edge" is used to differentiate companies at the core of the intranet infrastructure from those that operate at the edge. *See Tech Explained: The Glossary*, CTR. DEMOCRACY & TECH. (July 31, 2018), https://cdt.org/insights/tech-explained-the-glossary/ [https://perma.cc/8LR5-AWPA].

115. Social Media Privacy Protection and Consumer Rights Act of 2018, S. 2728, 115th Cong. (2d Sess. 2018).

116. *See generally* Data Care Act of 2018, S. 3744, 115th Cong. (2d Sess. 2018).

117. *Id.* § 3(a).

118. *See generally CDT Federal Baseline Privacy Legislation Discussion Draft Final*, CTR. DEMOCRACY & TECH. (2018), https://cdt.org/files/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf [https://perma.cc/J3HW-N8YP].

119. *Id.* § 5.

120. *See Innovative and Ethical Data Use Act of 2019*, INTEL (2019), https://usprivacybill.intel.com/wp-content/uploads/IntelPrivacyBill.pdf [https://perma.cc/CGV5-TBJK].

tions such as Access Now,[121] Business Roundtable,[122] The Software Alliance,[123] Electronic Privacy Information Center,[124] Google,[125] Internet Association,[126] Information Technology Industry Council,[127] and the U.S. Chamber of Commerce,[128] have all published frameworks and recommendations for federal privacy legislation as well. Mentions of consent in these bills and frameworks largely follow notice and choice models defining consent in the context of terms of service. Individuals are afforded greater transparency, but the representation of their true wishes is restricted to agreeing or disagreeing with a company's policies.

Indications of a more encouraging future for DNT might also be found in recent legal decisions regarding an individual's right to privacy. Back in 2012, Stanford University student Jonathan Mayer, now a faculty member at Princeton, published a report revealing loopholes that Google had exploited to track users' online behavior.[129] Despite the company's assurances that cookie settings would be respected, and despite their own promotion of an opt-out cookie blocker in Safari, Google had secretly coded web browsers to enable third-party tracking for years.[130] Mayer's report gained widespread attention, and soon, a group of users filed a lawsuit against the company, claiming violations under the Wiretap Act, Stored Communications Act, Computer Fraud and Abuse Act, California Invasion

121. *See Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers*, ACCESS NOW 1, 6–20 (2018), https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf [https://perma.cc/3B78-KXCF].

122. *See* Julie Sweet, *Business Roundtable Letter on Developing the Administration's Approach to Consumer Privacy*, BUS. ROUNDTABLE (Nov. 9, 2018), https://www.businessroundtable.org/business-roundtable-letter-on-developing-the-administrations-approach-to-consumer-privacy [https://perma.cc/5ETB-EXGN].

123. *See BSA Privacy Framework*, BSA: SOFTWARE ALLIANCE 1, 1–2 (2019), https://www.bsa.org/sites/default/files/2019-03/BSA_2018_PrivacyFramework.pdf [https://perma.cc/3ZAD-HF8H].

124. *See generally Draft Framework for Data Protection in the United States from Consumer and Privacy Organizations*, EPIC (2018), https://epic.org/testimony/congress/CPOs_to_SCC_US_Data_Protection_Framework_Oct2018.pdf [https://perma.cc/7P6B-XTDM].

125. *See generally Framework for Responsible Data Protection Regulation*, GOOGLE (2018), https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf [https://perma.cc/8JJE-JKYN].

126. *See generally IA Privacy Principles for a Modern National Regulatory Framework*, INTERNET ASS'N (2018), https://internetassociation.org/wp-content/uploads/2018/09/IA_Privacy-Principles-For-A-Modern-National-Regulatory-Framework_full-doc.pdf [https://perma.cc/KFA5-W4GK].

127. *See generally Framework to Advance Interoperable Rules (FAIR) on Privacy*, INFO. TECH. INDUSTRY COUNCIL (2018), https://www.itic.org/public-policy/FINALFrameworktoAdvanceInteroperableRules%28FAIR%29onPrivacyFinal_NoWatermark.pdf [https://perma.cc/878F-EECM].

128. *See generally U.S. Chamber Privacy Principles*, U.S. CHAMBER COM. (2018), https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf [https://perma.cc/S8XT-MJCN].

129. *See* Jonathan Mayer, *Safari Trackers*, WEB POL'Y (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/ [https://perma.cc/N9B6-B6BW]; *About*, JONATHAN MAYER, https://jonathanmayer.org [https://perma.cc/4UQD-BV7X].

130. *See* Mayer, *supra* note 129.

of Privacy Act, California Computer Crime Act, California Consumer Legal Remedies Act, California Unfair Competition Law, California tort law, and the California Constitution.[131] A Delaware district court judge dismissed all nine claims in 2013.[132] The Third Circuit, however, vacated the dismissal of the claims arising under California tort law and the California Constitution.[133] The decision cited the offensiveness of Google's actions and the user's right to privacy, writing: "Users are entitled to deny consent."[134] The case was then settled, leaving much to the legal imagination.[135]

In another showing of the power of state privacy law, the Illinois Supreme Court upheld an individual's right to deny consent in a critical decision regarding biometric data.[136] Ruling that Six Flags must pay damages for collecting a young boy's fingerprint without his permission, the court set the tone for future privacy cases.[137] The decision came at a time when courts across the state debated whether a party could be held liable for the collection of biometric information under Illinois' Biometric Information Privacy Act (BIPA)[138] if no injury or harm was shown, or if collection itself was enough. The court's ruling took a firm stance on the latter and will undoubtedly have a lasting impact on the legal world of user consent.[139]

II. European History of "Do Not Track"

Europeans are plagued by cookies as well, of course, but they have been far more willing to legislate the issue and are less interested in technical specifics. Cookies trigger two separate fundamental rights in Europe: privacy and data protection. The Council of Europe's European Convention on Human Rights of 1953 provides a "[r]ight to respect for privacy and

131. *See In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 443–51 (D. Del. 2013).

132. *Id.* at 451.

133. *See In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 153 (3rd Cir. 2015).

134. *Id.* at 151.

135. Though the settlement approved in February 2017 by U.S. District Judge Sue Robinson in Delaware has been successfully challenged. In a unanimous decision, the Third Circuit was particularly concerned about the cypres awards to the privacy groups funded by Google. *See generally In re* Google Inc. Cookie Placement Consumer Privacy Litig., 934 F.3d 316 (3rd Cir. 2019).

136. *See* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).

137. *Id.*

138. *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/ (2008).

139. One example can be found in the recent 2015 decision by the Ninth Circuit where Plaintiff Nimesh Patel sued Facebook for harvesting mapped facial data on photos uploaded to the site. Patel argued that the company did not obtain his consent to collect the data and was not transparent in the details of the data storage and usage. Though Facebook claimed that, without economic injury, Patel had no standing to sue, the Ninth Circuit rejected the company's arguments. The Illinois judgement served as the basis for the Court's decision and helped advance a $35 billion lawsuit against Facebook. Though the decision does not explicitly comment on "Do Not Track," its expanded definitions of injury promises to challenge the similar defenses that Facebook has built up against user consent in cookie tracking. *See generally* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

family life."[140] Article 8 of the Convention reads:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[141]

Additionally, the 2000 Charter of the Fundamental Rights of the European Union protects the right to private and family life in Article 7 and also provides a right to the protection of personal data in Article 8.[142]

Article 7 states, "[e]veryone has the right to respect for his or her private and family life, home and communications."[143] Article 8 states:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.[144]

The Charter was originally a political document intended to recognize a synthesized set of national and international obligations, but it became legally binding in 2009 under the Lisbon Treaty and now requires that all duties fulfilled by EU entities be done so within the bounds of the Charter.

The 1995 Data Protection Directive was initiated in 1990 by a communication from the European Commission and was specifically tied to a limitation of and enthusiasm for the European Single Market.[145] The integration that had begun in the 1950s with the 1957 Treaty of Rome (or the Treaty Establishing the European Economic Community (EEC)), waned with the economic decline of the 1970s, but was revitalized in the 1980s with leadership focused on market reforms.[146] The Single European Act of

---

140. Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, E.T.S. No. 5, 213 U.N.T.S. 222 [hereinafter ECHR].

141. *Id.*

142. Charter of the Fundamental Rights of the European Union, 2000 O.J. (C/ 364) 1, arts. 7–8.

143. *Id.* at art. 7.

144. *Id.* at art. 8.

145. Council Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter DPD 95/46].

146. *See How Maastricht Changed Europe: New Tools for a New European Agenda*, EUR. COUNCIL, https://www.consilium.europa.eu/en/maastricht-treaty/ [https://perma.cc/F224-3HQY] (last visited June 10, 2020).

1987 was the first major revision of the EEC and was dedicated to establishing an internal EU market by the end of 1992.[147] With little legal harmonization occurring under the Council of Europe's 1981 *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* (Convention 108) and the Organization for Economic Cooperation and Development's (OECD) *Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data*, the Commission was justified under these new political circumstances in proposing a directive "to ensure the establishment and functioning of the Internal Market," under the power granted in Article 100(a) of the EEC.[148] The draft of the Data Protection Directive was issued by the Commission in September of 1990,[149] heavily amended by Parliament in March 1992, redrafted with the addition of the "Free Movement of Such Data" months later,[150] and then heavily negotiated with the Council of the EU for two years.[151]

The basic structure of the final Data Protection Directive published in 1995 required EU member states to implement data protection laws that established six legal bases for processing data,[152] including consent of the data subject, as well as a number of additional data practice obligations and data subject rights.[153] Consent must be unambiguously given under the 1995 Directive, which was defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[154] It said little else about the matter.

The Telecommunications Directive, which would eventually become the EU Cookie Directive almost twenty years later, was proposed as a *lex specialis* together with the Data Protection Directive, a *lex generalis*, to "particularise and complement" the latter.[155] Although it was adopted in 1997, its implementation was stalled by the European Commission's review of regulatory approaches to electronic communication in 2000, which

147. *See generally* Single European Act, arts. 13, 29, 1987 O.J. (L 169) 1, 7, 13.

148. *Id.* at art. 17.

149. *Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data*, at 3, COM (1990) 314 final (July 27, 1990).

150. *Commission Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Market of Such Data*, at 30, COM (1992) 422 final (Oct. 16, 1992).

151. *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 445 (1995).

152. DPD 95/46, *supra* note 145, at art. 7(a). The other five legal bases are when: (1) processing is necessary to satisfy a contract to which the data subject is a party; (2) you need to process the data to comply with a legal obligation; (3) you need to process the data to save somebody's life; (4) processing is necessary to perform a task in the public interest or to carry out some official function; (5) there is a legitimate interest to process someone's personal data that does not infringe on the fundamental rights and freedoms of the data subject. *Id.* at art. 7(b)–(f).

153. *Id.* at art. 7(a)–(f).

154. *Id.* at art. 2(h).

155. Council Directive 97/66, of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, art. 1(2), 1997 O.J. (L 24) 1,4 [hereinafter Council Directive 97/66].

resulted in a call to replace the Telecommunications Directive, which focused on traditional telephone services, with a "technology neutral" approach that also reached electronic networks and services.[156] This led to the ePrivacy Directive which was adopted in 2002 and applies to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the [European] Community,"[157] including public communications networks supporting data collection and identification devices. Electronic communications services are defined in Article 2(c):

> '[E]lectronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, 101 which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.[158]

This distinction means that the ePrivacy Directive, which is still in force, applies to telecommunications operators and internet service providers but not to "information society services," such as platforms or apps (sometimes referred to as "over the top" services).[159] Nonetheless, Article 5(3), relating to access to information on a device (such as cookies placed on users' devices for later retrieval), and Article 13, relating to unsolicited communications, apply to all entities. Moreover, both, Article 5(3) and Article 13, require consent and cannot rely on other legal bases found in the GDPR or elsewhere.[160] Consent is defined in the ePrivacy Directive by reference to its definition in the Data Protection Directive (and now the GDPR) and has been a contentious aspect of the policy between the European Parliament and the Council of the EU for decades.[161]

The proposal by the European Commission contained no provisions specifically relating to cookies. A prohibition was introduced by the European Parliament's first reading of the proposal, in particular that, "[t]he use of devices to store information or to gain access to information stored in the terminal equipment of a subscriber (such as cookies) should be prohibited unless a prior explicit, well-informed and freely given consent of the

156. *Proposal for a Directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, at 225, COM (2000) 385 final (Aug. 25, 2000).

157. Council Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, art. 3, 2002 O.J. (L 201) 37, 43 (EC) [hereinafter ePrivacy Directive 2002/58].

158. Council Directive 2002/21, of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), art. 2(c), 2002 O.J. (L 201) 37, 43 (EC).

159. *Id.*

160. ePrivacy Directive 2002/58, *supra* 157, at arts. 5(3), 13.

161. *Id.* at 38.

users concerned has been obtained."[162] In February 1999, the A29WP issued a recommendation on "invisible and automatic processing of personal data on the internet performed by software and hardware," which states that users should be given clear notice and easy tools to exercise the option to accept or reject cookies, but that "[b]rowser software should, by default, be configured in such a way that only the minimum amount of information necessary for establishing an Internet connection is processed. Cookies should, by default, not be sent or stored."[163]

The Lisbon European Council (the Council) in 2000 set a goal to make Europe "the most competitive, knowledge-based economy in the world" by 2010, and did not want to risk driving Europeans away from e-commerce.[164] The Interactive Advertising Bureau (then the Internet Advertising Bureau), in the United Kingdom (U.K.), and the Federation of European Direct Marketing, along with others, organized an effective lobbying effort aimed at the Council's working group and the European Commission to change the amendment before its second reading. The European Commission offered an opt-out approach to the Council's working group, but the Council added that prior notice about the purposes of cookies should be given, as well as a right to refuse cookies, and added Recital 25 to further articulate its position.[165] This was not opt-in exactly but could have had similar consequences for site design and users. Ultimately, Article 5(3) of the 2002 ePrivacy Directive states:

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the *right to refuse* such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.[166]

The justification for the amendments to Recital 25 explain that, "cookies enhance surfing experience and provide for effective web services.

---

162. *Second Report on the Proposal for a Directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, at amend. 26, COM (2000) A5-0374/2001 final (Oct. 24, 2001).

163. *Recommendation 1/99 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware*, EUROPA 1, 1, 3, (1999), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf [https://perma.cc/C4F3-4WEW].

164. Börje Johansson et al., *The Lisbon Agenda from 2000 to 2010*, 13 (CESIS, Paper No. 106, 2007), http://www.diva-portal.org/smash/get/diva2:487429/FULLTEXT01.pdf [https://perma.cc/VE22-NB7D].

165. ePrivacy Directive 2002/58, *supra* 157, at 39.

166. *Id.* at art.5(3) (second emphasis added).

Clear and comprehensive information will enable consumers to make an informed choice. In addition, the means to accept and/or reject cookies already exist in most browser software."[167] Efforts of advertising and marketing lobbyists were met with little resistance from privacy advocates who were more focused on spam at the time. The compromise struck between the Parliamentary Committee (which wanted to restrict member states from implementing long and loose data retention policies) and the European Commission (which wanted to ban spam, and saw cookie restrictions as a hindrance to European competitiveness in e-commerce) was coordinated by the U.K. and its Benelux allies on the Council who lifted their opposition to an European-wide ban on spam in exchange for wording Article 5(3) so as to require "advance[d] notice."[168]

In 2003, Sony/BMG began downloading rootkits without consent when users inserted one of the company's MediaMax CDs. The Digital Rights Management software was not covered well by the ePrivacy Directive because an electronic communications network was not used.[169] Because of Sony's actions, the European Commission began the task of broadening Article 5(3) after an investigation by the U.K.'s National Consumer Council in 2006.[170] In 2009, the ePrivacy Directive had to be amended to address online tracking and is now referred to as the EU Cookie Directive.[171] This was not the original intention. In 2007, the European Commission issued a proposal for an updated ePrivacy Directive (this was done within the Citizens' Rights Directive) to broaden Article 5(3) beyond electronic networks but did not intend on changing the nature of the provision otherwise.[172] Nevertheless, the European Parliament saw the opportunity and took it. In the first reading, the European Parliament proposed Amendment 128, which read as follows:

---

167. *Recommendation for Second Reading on the Council Common Position for Adopting a European Parliament and Council Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, at 22, COM (2002) A5-0130/2002 final (Apr. 22, 2002).

168. Sylvia Mercado Kierkegaard, *How the Cookies (Almost) Crumbled: Privacy & Lobbyism*, 21 COMPUTER L. & SECURITY REP. 310, 320–21 (2005).

169. Kosta, *supra* note 30, at 384–85.

170. *Id.*

171. *See generally* Directive 2009/136, of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11 (EC) [hereinafter Cookie Directive 2009/136].

172. *Proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Consumer Protection Cooperation*, at 2–3, COM (2007) 698 final (Nov. 13, 2007) (making no change to the requirement that the user be provided with clear and comprehensive information).

> Member States shall ensure that the storing of information, or gaining access to information already stored, in the terminal equipment of a subscriber or user, either directly or indirectly by means of any kind of storage medium, is prohibited unless the subscriber or *user concerned has given his/her prior consent, taking into account that browser settings constitute prior consent, and is provided with clear and comprehensive information* in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing, and is offered the right to refuse such processing by data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.[173]

The European Commission rejected this amendment, but in the second reading, the European Parliament tried again. It kept the wording of consent in Article 5(3), but with a lighter tone:

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or *user concerned has given his/her consent, having been provided with clear and comprehensive information*, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[174]

The clarification that browser settings constituted consent or a lack of consent was removed to Recital 66, which stated, "[t]he user's consent to processing may be expressed by using the appropriate settings of a browser or other application."[175] These amendments were accepted by the European Council and Commission, but before the final signing of the new directive, thirteen members of the European Council commented in an Addendum, "[a]s indicated in [Recital 66], amended Article 5(3) is not intended to alter the existing requirement that such consent be exercised as a right to refuse the use of cookies or similar technologies used for legitimate purposes."[176] Recital 66 made reference to "clear and comprehensive information" and a "right to refuse," thus the group of European Council

173. Legislative Resolution of 24 September 2008 on the Proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Consumer Protection Cooperation, 2008 O.J. (C 8 E) 359, 386 (emphasis added).

174. Cookie Directive 2009/136, *supra* 171, at 30.

175. *Id.* at 20.

176. Council of the European Union, *Adoption of the Proposal for a Directive of the European Parliament and of the Council Amending Directives 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, and 2002/20/EC on the Authorisation of Electronic Communications Networks and Services (LA + S) (third reading)*, 15864/09 (Nov. 18, 2009), *available at* https://register.consilium.europa.eu/doc/srv?l=en&f=st%2015864%202009%20ADD%201%20REV%201 [https://perma.cc/RB8X-VDJA].

members interpreted a right to refuse as consent, which was essentially the same opt-out system in place from the 2002 ePrivacy Directive.[177] The A29WP did not have the same interpretation. It found two distinct conditions in the 2009 version of Article 5(3). Namely, an obligation to obtain consent, and an obligation to provide clear and comprehensive information. In fact, the A29WP (disbanded and replaced by the Data Protection Board under the GDPR) drafted guidance every year for four years on cookies and consent.[178] But variations on consent and browser settings remain among national legislation.[179] These inconsistencies were seen as a problem to the Single Market and to the fundamental rights of Europeans.

In 2009, the European Commission also announced its interest in creating EU data protection laws that would update the Data Protection Directive and would be substantively binding and consistent across all member states.[180] The Lisbon Treaty granted the Charter more than just a binding legal status; it also granted the EU a legal basis for comprehensive data protection legislation across the European Community.[181] Prior to the agreement, the EU only had the internal market as a legal basis, which could only justify directing national laws to approximate one another so as to not inhibit the free flow of data across borders. In January 2012, the European Commission published its proposal, and in doing so, started the

177. Cookie Directive 2009/136, *supra* 171, at 20.

178. Article 29 Data Prot. Working Party, *Opinion 2/2010 on Online Behavioural Advertising*, WP 171 (June 6, 2010), *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf [https://perma.cc/79DY-L38X]; Article 29 Data Prot. Working Party, *Opinion 15/2011 on the Definition of Consent*, WP 187 (July 13, 2011), *available at* https://www.pdpjournals.com/docs/88081.pdf [https://perma.cc/PW3F-8WHT]; Article 29 Data Prot. Working Party, *Opinion 04/2012 on Cookie Consent Exemption*, WP 194 (June 7, 2012), *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf [https://perma.cc/W3CU-PJKH]; Article 29 Data Prot. Working Party, *Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies*, WP 208 (Oct. 2, 2013), *available at* https://www.pdpjournals.com/docs/88135.pdf [https://perma.cc/B7G6-3NFV].

179. *See, e.g.*, *Guidance on the Rules on Use of Cookies and Similar Technologies*, ICO 1, 6 (2012), https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf [https://perma.cc/J8FL-TWQU] (requiring prior consent based on the change to 5(3)); *but see* Telecommunicatiewet 4 februari 2015, Stb. 2015, artikel 11.7(a)(1) (enacting a strict Dutch law in 2013 that deemed default privacy settings in the browser unacceptable forms of user consent—it was so unpopular that amendments were sought in 2014 and passed in March 2015). *See generally* Ronald Leenes & Eleni Kosta, *Taming the Cookie Monster with Dutch Law—A Tale of Regulatory Failure*, 31 COMPUTER L. & SECURITY REV. 317 (2015); Robert Bond, *The EU E-Privacy Directive and Consent to Cookies*, 68 BUS. LAW. 215 (2012); Joasia Luzak, *Much Ado About Cookies: The European Debate on the New Provisions of the ePrivacy Directive Regarding Cookies*, 21 EUR. REV. PRIV. L. 221 (2013). Updated details of each country's cookie laws can be found on the Interactive Advertising Bureau's website. *See Europe's Cookie Laws: E-Privacy Directive Implementation Center*, IAB, https://web.archive.org/web/20160617122010/https://www.iabeurope.eu/eucookielaws [https://perma.cc/M5DT-M2DT] (last visited June 10, 2020).

180. *The Protection of Fundamental Rights in the EU*, EUR. PARLIAMENT, https://www.europarl.europa.eu/factsheets/en/sheet/146/the-protection-of-fundamental-rights-in-the-eu [https://perma.cc/YCQ8-3K3Y] (last visited June 11, 2020).

181. *Id.*

EU legislative process with the European Parliament and Council. The European Parliament published the agreed-upon language in Spring of 2014; and the European Council published it in 2015. The GDPR was officially published in April of 2016 and—to much international fanfare—went into effect May 25, 2018.[182] Most relevantly, the GDPR changed consent as a legal basis for processing personal data, making it a much less attractive option from the list of six.[183]

One of the main shifts the GDPR accomplished was changing the meaning of consent, but the definition in Article 4(11) remains largely intact: "'[C]onsent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her . . . ."[184] The power of consent is further reinforced by Article 7, which requires the data controller to demonstrate a proof of consent, establishes a right to withdraw consent (further expanded upon in Recital 42), and states that consent must be clearly distinguishable from other matters and be consistent with all requirements of the GDPR.[185] Recital 32 removes the possibility of opt-out consent by prohibiting silence, inactivity, and pre-ticked boxes as sufficient evidence of affirmative consent.[186] Recital 32 also states that the data subject may "choos[e] technical settings for information society services" as a means of consent, but the specificity requirement creates a challenge for existing browser settings.[187] The "Do Not Track" header probably does not meet this requirement. The A29WP 2017 guidance on consent mentions browsers only once and briefly explains:

> An often-mentioned example to do this in the online context is to obtain consent of Internet users via their browser settings. Such settings should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers.[188]

The GDPR does not intend to address the specifics of browser settings and cookies. In January 2017, the European Commission proposed the ePrivacy Regulation to harmonize member states in their implementation and alignment with the GDPR. As with its prior directive versions, the ePrivacy Regulation is notably *lex specialis*, meaning it overrides the *lex generalis* GDPR for specific areas.[189] The proposal does many things

182. *The History of the General Data Protection Regulation*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [https://perma.cc/W4B5-9UYY] (last visited June 11, 2020).
183. GDPR, *supra* note 2, at art. 6(1)(a).
184. *Id.* at art. 4(11).
185. *Id.* at art. 7.
186. *Id.* at 6.
187. *Id.*
188. A29WP Guidelines, *supra* note 7, at 17.
189. Council Directive 97/66, *supra* note 155, at art. 1(2).

including mandating consent before saving and accessing cookies at the browser level,[190] and explaining the lack of need for consent to access cookies used as session-IDs to: (1) keep track of online forms and shopping carts (limited to a session or a few hours); (2) enable playback for multimedia content players (a session); (3) authenticate users as logged in (a session), or for security purposes (limited duration); (4) customize user interface like language settings (a session); and (5) authenticate users as logged in to social networks sites.[191] There are no exceptions for fulfilling contracts or arguing legitimate interests.

When the European Council, under the Austrian Presidency, published its revised draft of the ePrivacy Regulation in July 2018, Article 10 was gone and every instance of the word "browser" was crossed out. The draft explained that Article 10 had

> raised a lot of concerns, including with regard to the burden for browsers and apps, the competition aspect, the link to fines for non-compliance but also the impact on end-users and the ability of this provision to address e.g.[,] the issue of consent fatigue, thus raising doubts about its added value. . . .[192]

The October 2019 draft stated that individual consent with individual websites and services (e.g., cookie banners, pop-ups, windows) would remain the legally enforceable way to administer cookies and data tracking across the web. The draft also included more exceptions for cookies that do not

---

190. A29WP Guidelines, *supra* note 7, at 17. A29W's support for the European Commission's review and revision of the ePrivacy Directive also encouraged consent at the browser level:

> When consent is the applicable legal basis, users must be provided with truly easy (user friendly) means to provide and revoke consent. The Working Party recommends rephrasing the requirements in the current Recital 66 of Directive 2009/136/EC. Instead of relying on website operators to obtain consent on behalf of third parties (such as advertising and social networks), manufacturers of browsers and other software or operating systems should be encouraged to develop, implement and ensure effective user empowerment, by offering control tools within the browser (or other software or operating system) such as Do Not Track (DNT), or other technical means that allow users to easily express and withdraw their specific consent, in accordance with Article 7 of the GDPR. Such tools can be offered to the user at the initial set-up with privacy-friendly default settings.

E-mail from Rob van Eijk, Founder & Dir., Blaeu, to Mike O'Neill, Co-Founder & CTO, Baycloud, and Matthias Schunter, Principal Eng'r, Intel (July 26, 2016 2:56 PM), *available at* https://lists.w3.org/Archives/Public/public-tracking/2016Jul/0026.html [https://perma.cc/DZ9U-DGF4].

191. *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 10 final (Oct. 1, 2017) [hereinafter *Proposal* COM (2017)].

192. Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2003/58/EC (Regulation on Privacy and Electronic Communications)*, 10975/18 (July 10, 2018), *available at* http://data.consilium.europa.eu/doc/document/ST-10975-2018-INIT/en/pdf [https://perma.cc/MKK2-5854].

need consent, such as fraud detection, security, and statistics.[193]

No more work was expected to occur around the ePrivacy Regulation until the European Parliament elections in May 2019, and after the Romanian Presidency of the European Council was handed off to Finland in July.[194] In fact, the EU telecommunication ministers met in early June but made no public progress.[195] Cookies, and the economics of web consent, are only part of the negotiations. Accessing electronic communications is another, as well as IoT devices and connected cars.[196] The Finnish presidency has emphasized digital strategy, economic growth, and job creation: "During its Presidency of the Council of the EU, Finland aims to boost the growth of the data economy and the utilisation of artificial intelligence as part of developing the European single market. The data economy should be driven by the consumer, in other words by the user."[197] Under the motto "[s]mart connections for sustainable growth,"[198] the Finnish delegation further explained:

> We wish to turn the discussions toward trusted and human-centric data economy within Europe, respecting the rights and privacy of individuals. Throughout our presidency and through high-level conferences on data and digital transport, we aim to involve businesses, stakeholders and citizens alike in the discussions on European data policy. Our aim, too, is to encourage debate on what can be done to promote the access to and the reuse of data in general, in the context of sectoral development and with regard to AI. We will also continue the negotiations on the ePrivacy proposal and further them as far as possible with the aim to ensure high quality of the legislation.[199]

GDPR enforcement has addressed consent that occurs between sites and services collecting and processing personal data. For instance, on January 21, 2019, the French data protection agency (CNIL) imposed a fine of fifty million euros against Google for its personalized ad practices, which, the agency determined did not meet the standards for valid consent because users were not sufficiently informed since the disclosure was neither specific nor unambiguous.[200] On October 1, 2019, the Court of

193. *See generally Proposal* COM (2017), *supra* note 191.

194. David Thomas, *ePrivacy Regulation Continues to Stall, but There's Hope?*, IAPP (June 12, 2019), https://iapp.org/news/a/eprivacy-regulation-continues-to-stall-but-theres-hope/ [https://perma.cc/RB7S-WUCU].

195. *Video Conference of Telecommunications Ministers, 5 June 2020*, EUR. COUNCIL (June 5, 2020), https://www.consilium.europa.eu/en/meetings/tte/2020/06/05/ [https://perma.cc/G6A2-5GBX].

196. *Id.*

197. *Data Economy*, EU2019.FI, https://eu2019.fi/en/backgrouders/data-economy [https://perma.cc/5K5T-L9BN] (last visited June 10, 2020).

198. Council of the European Union, *Work Programme of the Incoming Presidency*, Telecom 241 9677/19 (May 27, 2019), *available at* https://data.consilium.europa.eu/doc/document/ST-9677-2019-INIT/en/pdf [https://perma.cc/AE3P-QL8Y].

199. *Id.*

200. *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc [https://perma.cc/8VS8-WSR5].

Justice of the European Union (CJEU) handed down a judgement in the "Planet49 case." The Planet49 case was referred to the CJEU by a German Court asking for guidance on: (1) pre-checked boxes for cookie placement, (2) whether the personal nature of the data mattered, and (3) the requirements for the duration of cookies in the notification. In interpreting Article 5(3) of the ePrivacy Directive, the CJEU concluded that pre-checked boxes do not constitute valid consent, that expiration dates on cookies should be disclosed, and that different purposes could not be bundled into the same consent request. The court also confirmed that these rules apply to cookies irrespective of whether the data is personal or not.[201]

III. Protecting Non-Use

During his testimony, Zuckerberg repeatedly insisted that users have a great deal of control on Facebook. In response to a question from a Congressman regarding user privacy, Zuckerberg said:

> [O]n Facebook, you have control over your information. The content that you share, you put there. You can take it down at any time. The information that we collect, you can choose to have us not collect. You can delete any of it. And, of course, you can leave Facebook if you want.[202]

Many of the first privacy scholars, in their writings in the mid-to-late twentieth century, called for the re-orientation, or perhaps evolution, of privacy to reflect this type of individual control.[203] This suited the changes to concepts like the individual, the citizen, the consumer, the student, etc.,[204] as well as to the growing distrust of the government and corporate powers after the Cold War when consensus began to wane,[205] and the concept of information, or data having monetary value and being a possessory object, took shape in public.[206]

However, privacy as individual consent and control took several decades to take hold and did not enter policy debates until the 1980s and 1990s.[207] At that time, the OECD adopted guidelines stating that personal data should not be disclosed or used for unspecified purposes unless user consent was obtained.[208] Several years later, the Data Protection Directive included similar rules for processing personal data with unambiguous user

201. Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, 2019 E.C.R. ¶ 82.

202. Zuckerberg Hearing, *supra* note 1.

203. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 32-46 (Univ. Mich. Press 1971); ALAN F. WESTIN, PRIVACY AND FREEDOM 349-63 (Atheneum 1967).

204. *Cf.* SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 60-63, 73 (Harvard Univ. Press 2018); DAVID VINCENT, PRIVACY: A SHORT HISTORY 113, 128-29 (Polity Press 2018).

205. THOMAS P. HUGHES, RESCUING PROMETHEUS: FOUR MONUMENTAL PROJECTS THAT CHANGED THE MODERN WORLD 303-04 (Vintage Books 1998) (1957).

206. Sarah E. Igo, *Me and My Data*, 48 HIST. STUD. NAT. SCI. 616, 619 (2018).

207. Meg Leta Jones, *The Development of Consent to Computing*, IEEE ANNALS HIST. COMPUTING, Oct.-Dec. 2019, at 34, 39-42.

208. *Id.* at 42.

consent under Article 7.[209] After the concept of control was integrated into data protection regimes, privacy laws, and best practices in various ways, contemporary privacy scholars and researchers reinforced control by spending another decade trying to achieve the type and system of control that resulted in meaningful privacy built on notice and consent.

Since then, many, if not most, have given up on control. As early as 2006, Fred Cate articulated the unsatisfactory privacy interest based on "mere notice and consent."[210] Solon Barocas and Helen Nissenbaum, in 2009, asserted the need for "substantive direct regulation"[211] in the context of targeted advertising. In 2012, Ryan Calo published *Against Notice Skepticism in Privacy (and Elsewhere)* to respond to the growing tide of privacy commentators prepared to abandon notice and choice regulatory mechanisms.[212] Most recently in the U.S., Woodrow Hartzog, for instance, criticized privacy regimes like the GDPR and ePrivacy Directive for their commitment to control,[213] lamenting his own efforts:

> I'm guilty of it too. In the past I've advocated for more control over personal information. I've sought private law approaches that might empower data subjects and meaningfully mitigate data abuses. I now realise that I was asking far too much from a concept that works best when preserved, optimized, and deployed in remarkably limited doses. Our personal agency is required for control to work and, after all, we are only human. The concept of control is far too precious and finite to meaningfully scale. It will never work for personal data mediated by technology.[214]

Invoking Cass Sunstein's "choice architecture,"[215] Hartzog goes on to explain that control is all about design and that platform designs limit and manipulate our choices to maximize disclosure. This is based on research that reveals the pathetic state of the user. The user is central to the way technology is imagined, conceptualized, designed, integrated, and regulated. Joseph Turow and his co-authors have surveyed the landscape for years, finding that users continue to interpret the existence of a privacy policy on a website as protection of privacy.[216] Lorrie Cranor, along with

---

209. *Id.*

210. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 357 (Jane K. Winn ed., Ashgate Publ'g 2006) (discussing the failure of the notice and choice model to meaningfully protect privacy).

211. Solon Barocas & Helen Nissenbaum, On Notice: The Trouble with Notice and Consent 6 (Oct. 2009) (unpublished manuscript), *available at* https://nissenbaum.tech.cornell.edu [https://perma.cc/4FBY-QB27].

212. *See generally* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012).

213. Whether or not such a commitment to control exists is another question.

214. Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROTECTION L. REV. 423, 426 (2018).

215. *See generally* Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. REG. 413 (2015) (arguing that all people make all of their decisions within an architecture that affects both intentional and non-intentional choices).

216. *See* Joseph Turow et al., *Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003-2015*, 62 J. BROADCASTING & ELECTRONIC MEDIA 461, 463 (2018).

various co-authors, researched user understanding and the meaning of privacy policy content,[217] and have tested a number of labeling schemes[218] and education strategies.[219] Alessandro Acquisti and Cranor are leading behavioral economists who have discussed why users state their value in, and prioritize, privacy, yet these users take actions counter to such claims.[220] The FTC has been very interested in these studies and findings, and Chairman Leibowitz acknowledged that the notice and choice model fails to properly protect privacy precisely because of this reliance on the user to control their own data.[221] Scholars that have created evidence of how users struggle have also emphasized the challenging power dynamics that users operate under. For example, Cranor and McDonald famously calculated how many hours per year it would take to read privacy policies alone.[222] Acquisti and Jens Grossklags argued that user behavior is rational when understood within the uncertainties, ambiguities, and complexities that characterize privacy choices in contemporary situations.[223] Nora Draper and Turow argued that corporate approaches to the user cultivate "digital resignation."[224]

We suggest that instead of focusing on "the user," who is a highly contested subject, we should focus on non-users. In 2003, Sally Wyatt articulated the need to account for non-users who are not potential users or not-yet users as much of the digital divide remains.[225] Wyatt sketched out a set of actors with multiple motivations categorizing four non-users: resisters, rejecters, excluded, and expelled. "Resisters" have never wanted to be

---

217. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *Americans' Attitudes About Internet Behavioral Advertising Practices*, *in* PROCEEDINGS OF THE 9TH ANNUAL ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 63, 67 (ACM 2010); Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 63–64 (2015).

218. *See* Patrick G. Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1573 (ACM 2010); Joseph Reagle & Lorrie Faith Cranor, *The Platform for Privacy Preferences*, COMM. ACM, Feb. 1999, at 48, 50.

219. *See generally* Lorrie Faith Cranor et al., *Empirical Evaluations of Embedded Training for Antiphishing User Education*, *in* MANAGING AN INFORMATION SECURITY AND PRIVACY AWARENESS AND TRAINING PROGRAM (CRC Press 2d ed. 2010).

220. *See generally* Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, IEEE SECURITY & PRIVACY, Nov.–Dec. 2009, at 82; Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 SCI. 509 (2015); Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELECTRONIC COMMERCE 31 (ACM 2004); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SECURITY & PRIVACY , Jan.–Feb. 2005, at 26.

221. Fred H. Cate, *The Limits of Notice and Choice*, IEEE SECURITY & PRIVACY, Mar.–Apr. 2010, at 59, 59.

222. *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 563 (2008).

223. *See generally* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363 (Alessandro Acquisti et al. eds., Auerbach Publ'n 2008).

224. Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 NEW MEDIA & SOC'Y 1824, 1829 (2019).

225. Wyatt, *supra* note 37, at 75–76.

online, "rejecters" have left voluntarily, and those who have been "excluded" or "expelled" are barred from access.[226] We are interested in the non-use that occurs by "rejecters" who previously "stopped using the internet voluntarily, perhaps because they find it boring or expensive or because they have perfectly adequate alternative sources of information and communication," but want to leave today for the same reasons, or for political reasons.[227]

The user versus non-user dichotomy has significant limitations that scholars promoting a more dynamic and spectral understanding of use have put forth. The bulk of studies on users has been on their *individual* perceptions, experiences, and actions. Acknowledging that human computer interaction has neglected non-users in *Beyond the User: Use and Non-Use in HCI*, Christine Satchell and Paul Dourish explain that "non-use is not an absence or a gap; it is not negative space. Non-use is, often, active, meaningful, motivated, considered, structured, specific, nuanced, directed, and productive."[228] Karen Levy points out that it is more fruitful to consider the user and non-user as a constellation of mutually constitutive people, organizations, and objects, and that the law and regulatory frameworks can and do "acknowledge[ ] the networked nature of sociotechnical relation to a degree not contemplated by theoretical models."[229] Privacy law has not done so. Although the EU has utilized a more networked discussion of data protection (e.g., the Data Protection Directive and GDPR are sophisticated representations), and explicitly grants a general right to object to data processing and a right to delete as means of non-use, the ePrivacy Regulation remains trapped in an individual user framing and does not acknowledge, support, or protect non-use.[230] Article 21(5) of the GDPR states that "the data subject may exercise his or her right to object by automated means using technical specifications,"[231] but the removal of Article 10 in the ePrivacy Regulation will override explanations expressed in the GDPR. Although the ePrivacy Regulation will require explicit consent, defined more meaningfully in the GDPR than in the previous directive, there is no protection for political or other types of non-use.[232]

The history of U.S. privacy moments is similarly blind to non-use, but this speaks more to the nature of American policy innovation. Few data protection laws have passed in the U.S. outside the context of social institutions that were regarded as desirable and necessary. This includes the Fair Credit Reporting Act (which covers data held by credit reporting agencies), the Privacy Act (which covers disclosure of personal data held by government agencies), Family Educational Rights and Privacy Act (which covers

226. *Id.* at 76.
227. *Id.*
228. Christine Satchell & Paul Dourish, *Beyond the User: Use and Non-use in HCI*, *in* PROCEEDINGS OF THE 21ST ANNUAL CONFERENCE OF THE AUSTRALIAN COMPUTER-HUMAN INTERACTION SPECIAL INTEREST GROUP 9, 15 (2009).
229. Karen E.C. Levy, *The User as Network*, FIRST MONDAY, Nov. 2015, at 1, 3.
230. ePrivacy Directive 2002/58, *supra* note 157.
231. GDPR, *supra* note 2, at art. 21(5).
232. ePrivacy Directive 2002/58, *supra* note 157.

student education records), and Health Insurance Portability and Accountability Act (which covers medical records held by health care providers).[233] Non-use is not built into these rules because they are only passed when non-use is seen as both, impossible *and* socially unbeneficial.

The U.S. has only recently begun to confront relatively new consolidations of power, limited choice, inevitability of some types of online engagement, and ideas of social benefit on the web. This debate is currently tangled up with some of these older "inevitable" and "beneficial" social institutions across a number of contested intertwined conflicts, scandals, and players. These include social media and antitrust debates; restrictions on the use of online services for certain felons; "screen time" for healthy children; personalized education; medicine; home-schooling; anti-vaxxers; government surveillance and leaks; platform policies limiting hate speech; financial justice; algorithmic bias; and technological diversity. However, non-use as a form of political resistance or economic choice is an important element of U.S. policy. While the political moment is quite chaotic, protection of an opt-out standard supports a type of American non-use.

Protecting non-use is quite different from protecting individual users by means of control. It is also distinct from attempts to protect third-party individuals who are implicated by the disclosures of others—what Mark MacCarthy called privacy externalities in 2011,[234] and what Levy and Barocas taxonomized as privacy dependencies in 2018.[235] Protecting non-use is protecting those that have chosen to not choose and to be a political non-user. Non-use is similar to Nissenbaum and Finn Brunton's *Obfuscation*, which is motivated by resistance and protest and serves as "a *user's* guide for privacy and protest."[236] It seeks to educate the public on how individuals can evade, protest, and sabotage today's pervasive digital surveillance by deploying more data, not less. Non-use seeks to protect the refusal that these authors assume is unavailable, unimportant, or ineffective in a very different political environment than they were writing in even a couple of years ago. The GDPR and new political motivations in the U.S. have created a new potential for non-use, understood in this instance as the legal enforcement of browser settings. By focusing on non-use, international interoperability is also made more obvious. In the most simplistic terms, the EU requires consent (or other moral/legal justification) to computationally access, collect, or process personal information, but the U.S.

233. *See Existing Federal Privacy Laws*, CTR. FOR DEMOCRACY & TECH. (Nov. 30, 2008), https://cdt.org/insights/existing-federal-privacy-laws/ [https://perma.cc/WL6B-D5SW]. Exceptions include rare instances where particular harms were perceived and strange political demands arose, as in the Video Privacy Protection Act and the privacy portions of the Gramm-Leach-Bliley Act (a.k.a. the Financial Services Modernization Act of 1999). *Id. See also, e.g.*, *The Gramm-Leach-Bliley Act*, EPIC, https://epic.org/privacy/glba/ [https://perma.cc/SNT3-UAXH] (last visited June 12, 2020).

234. *See generally* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6I/S: J.L. & POL'Y FOR INFO. SOC'Y 1, 5 (2011).

235. *See* Karen Levy & Solon Barocas, *Refractive Surveillance: Monitoring Customers to Manage Workers*, 12 INT'L J. COMM. 1166, 1167 (2018).

236. *See generally* FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (MIT Press 2015).

does not. Thus, browser settings in the EU may be opt-in, but may remain opt-out in the U.S.

The legislative understanding and rhetoric around notice and choice is still unclear. Although administrative agencies and legislators in the U.S. and Europe have made it clear that notice and choice currently "do[ ] not work," there is less consistency, often divided by party lines, in descriptions of how it is malfunctioning and whether policymakers are prepared to retire or supplement the regime. In the past, PETs like Google's "Keep My Opt-Outs" and Mozilla's TACO functioned as privacy protection for non-users but were limited by the lack of interoperability and enforcement. The W3C's quest to standardize DNT would have created a path for overcoming those obstacles, but without real political will from administrative or legislative actors, the organization's inability to retain the DAA as a stakeholder severed that chance. In a similar, slippery fashion, the EU was able to pass a directive (and amendments) that offered an imprecise mechanism for obtaining consent. Thus, today, consent in Europe has more stringent confines than those provided by the GDPR; nevertheless, uncertainty around browser settings continues due to the specificity requirements of consent.[237] While consent at the browser level was removed from the ePrivacy Regulation draft by the European Council in its most recent iteration, approval from the European Parliament is still pending and the removal will certainly be addressed.

Meanwhile, the vast majority of proposed privacy legislation in the U.S. continues to overlook non-users and, instead, relies on site, or service-specific, notice and choice models to protect privacy, with one real exception. Senator Ron Wyden's Consumer Data Protection Act attempts to resurrect non-use through its employment of DNT.[238] Section 6 of the bill would require the FTC to implement and maintain a website dedicated to an individual's tracking settings. With a simple switch, individuals could opt-out of all data sharing by covered entities to third parties and view or change their status at any time. Drawing on the DNT models of the past, Wyden's bill would require these features to be available through at least one technological mechanism, such as a web browser setting or through an individual's operating system.[239] But the bill would also go beyond DNT's mired history to give the tracking setting legal backing. Covered entities would be bound to an individual's DNT status by FTC enforcement.

Further, the Consumer Data Protection Act legitimizes an individual's right to choose by providing alternative solutions around the commonly employed "legitimate business interest" loophole.[240] While the vast major-

237. *See* Natasha Lomas, *Most EU Cookie 'Consent' Notices Are Meaningless or Manipulative, Study Finds*, TECHCRUNCH (Aug. 10, 2019, 9:00 AM), https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/ [https://perma.cc/2VRN-QUKL] (explaining the way developers and privacy researchers view the challenges between cookie notices and browser settings).

238. Consumer Data Protection Act, S. 2188, 115th Cong. § 6 (2d Sess. 2018) (discussion draft proposed by Sen. Ron Wyden).

239. *Id.*

240. *Id.* § 6(B)(i).

ity of privacy legislation currently proposed allows for covered entities to shirk consent requirements if their products or services necessitate data collection, Wyden's bill maintains an individual's DNT status.[241] Covered entities have the option to charge individuals monetarily or through other mechanisms in lieu of monetizing their personal information.

Introduced in a time when technology adoption is increasingly legislated as unavoidable, the Consumer Data Protection Act breathes life back into DNT as a tool for understanding the full ecosystem of individuals and technologies. Under this bill, legal hurdles plaguing cases like Google's cookie blocker lawsuit would be knocked down, and limited interpretations and applications of user consent and choice would be broadened. The bill would provide support for the judgments, like those surrounding BIPA, by allowing individuals the right to deny consent, but even more, establishing that a choice should be available. Use should not be assumed. Wyden's revival of DNT honors the non-user's choice to not choose and, in doing so, commits to giving legal teeth to the emerging cultural zeitgeist of individual consent and non-use as a form of resistance.

Just as they did during DNT's first life cycle and the ePrivacy Regulation drafts, advertisers and platforms offer their many arguments against blocking third-party or unnecessary cookies: a DNT mechanism would only push tracking into more invasive territory, or it might force websites into asking for payment from users.[242] While there are equally as many compelling, counter-arguments that invalidate these concerns, there still exist other, broader issues surrounding cookies and consent. An article published by *The Verge* in 2017 details Apple's new tracking settings for its Safari browser.[243] In a show of commitment to user privacy, Safari would block nearly all third-party trackers by default, limiting their use by third parties only if users had not interacted with the site from which they originated in the last twenty-four hours.[244] If that site had not been accessed in the last month, they would be altogether deleted.[245] However, as the article explains, "Google and Facebook are poised to come out of that game ahead."[246] Third-party advertisers originating from the data duopolies would carry on business as usual, as Google and Facebook are two of the sites most likely to be visited on a daily basis. But other third-party systems would find their cookies blocked and their advertisers turning to do business with Facebook and Google instead.[247]

Wyden's bill runs parallel with its third-party data sharing exception. Covered entities are entitled to share user data with third parties if it is

241. *See generally id.*
242. *Id.*
243. Russell Brandom, *Apple's New Anti-Tracking System Will Make Google and Facebook Even More Powerful*, VERGE (June 6, 2017, 1:56 PM), https://www.theverge.com/2017/6/6/15747300/apple-safari-ad-tracking-cookie-blocker-google-facebook-privacy [https://perma.cc/SBJ5-23Z6].
244. *Id.*
245. *Id.*
246. *Id.*
247. *Id.*

considered necessary for their service, and advertising is certainly made to fall into that consideration.[248] Though the bill does offer the option to pay a fee in lieu of consenting to data sharing, this choice still favors the powerful players. It is well-reported that many users are unwilling to pay anything to use even the most frequented sites like Facebook,[249] and most would likely be unwilling to pay what the platforms would have to charge to recoup lost advertising revenue. These individuals would choose to pay with their data for Facebook and Google while less-popular, competing sites would likely be abandoned entirely.

This front is also unclear in Europe. Although cookie walls that prevent access to sites have been declared non-compliant as coercive mechanisms for obtaining consent by the Dutch Data Protection Agency,[250] portions of sites or services may be walled off to those that block cookies according to Recital 25 of the 2002 ePrivacy Directive[251] and in the face of criticism from the A29WP.[252] This interplay between the GDPR and the ePrivacy Directive remains contested.[253] A more immediate concern is noncompliant browser settings that do not provide specific consent, and therefore, further the incessant cookie banners and pop-ups. However, once the technical specifications for particular browser settings are clear, European law is set up to legally support such non-use through the GDPR, but it will certainly need the clarity of a new ePrivacy Regulation because at the moment, neither the GDPR, nor the current ePrivacy Directive, are equipped to handle concerns of growing monopoly powers.

There is much to consider regarding consent, particularly the legitimacy of choice in these scenarios for those in lower socioeconomic classes, but the competition and antitrust implications of cookie blocking and plat-

248. *Id. See also* Consumer Data Protection Act, S. 2188, 115th Cong. § 6 (2d Sess. 2018) (discussion draft proposed by Sen. Ron Wyden).

249. Rani Molla, *How Much Would You Pay for Facebook Without Ads?*, VOX (Apr. 11, 2018, 5:46 PM), https://www.vox.com/2018/4/11/17225328/facebook-ads-free-paid-service-mark-zuckerberg [https://perma.cc/8THC-WUXD].

250. *Websites Must Remain Accessible if Tracking Cookies Are Refused*, AUTORITEIT PERSOONSGEGEVENS (2019), https://www.privacysecurityacademy.com/wp-content/uploads/2020/05/Netherlands_Cookie_update_March_2019.pdf [https://perma.cc/3L44-A8UA].

251. ePrivacy Directive 2002/58, *supra* note 157, at 39.

252. Article 29 Data Prot. Working Party, *Opinion 8/2006 on the Review of the Regulatory Framework for Electronic Communications and Services, with Focus on the ePrivacy Directive*, WP 126 (Sept. 26, 2006), *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp126_en.pdf [https://perma.cc/WJ49-69GH]; Article 29 Data Prot. Working Party, *Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies*, WP 208 (Oct. 2, 2013), *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf [https://perma.cc/EX48-S9U7].

253. Natasha Lomas, *Cookie Walls Don't Comply with GDPR, Says Dutch DPA*, TECHCRUNCH (Mar. 8, 2019, 5:37 AM), https://techcrunch.com/2019/03/08/cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/ [https://perma.cc/5439-WN8A]. *See also* Frederik J. Zuiderveen Borgesius et al., *Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation*, 3 EUR. DATA PROTECTION L. REV. 353, 361 (2017).

form subscriptions must also be addressed.[254] So far, the EU has been aggressively investigating, fining, and altering more large technology companies than the U.S.,[255] but whether or not to "break up Big Tech" has become a policy issue for Democratic 2020 presidential hopefuls.[256]

Conclusion

The California Consumer Privacy Act, set to take effect in the state on January 1, 2020, represents the growing opportunity for a national data protection law in the U.S. While the law gives California residents the right to opt-out of the sale of personal information and would prohibit businesses from discriminating against residents who exercise this right,[257] this requirement for individuals to make a choice follows the path set by the many other privacy bills that came before it. But the potential to move the privacy conversation forward and take non-use into consideration is as high as ever. In October 2019, Senator Wyden introduced the latest iteration of his Consumer Data Protection Act draft bill, naming it the Mind Your Own Business Act of 2019.[258] Sharing many similarities with his original plan, the Mind Your Own Business Act once again proposes a DNT mechanism that gives individuals the choice to not choose.[259] Meanwhile, GDPR enforcement actions around consent have reinforced a focus on the user, and promoted control, choice, and active choosing. While many privacy scholars have moved beyond notice, choice, and control, those three elements continue to be brought up in U.S. privacy debates and remain central to the EU's fundamental rights in data protection. Others have proposed more radical reconstructions of data privacy, like fiduciary relationships, but we propose a more modest and immediate shift—one that simply recognizes non-use as an important component of information practice.

254. One possible solution for mitigating these issues would be the expansion for alternative access. Instead of giving individuals the choice to pay by money or pay by data, websites might also offer the chance to gain access by improving its artificial intelligence. By selecting all of the traffic lights in a series of photos, users would feel less pressure to stay within a small and powerful fraction of the web, and advertisers would not feel compelled to leave their other third-party systems.

255. Elizabeth Schulze, *If You Want to Know What a US Tech Crackdown May Look Like, Check Out What Europe Did*, CNBC (June 7, 2019, 1:36 AM), https://www.cnbc.com/2019/06/07/how-google-facebook-amazon-and-apple-faced-eu-tech-antitrust-rules.html [https://perma.cc/R625-GWJU].

256. *Should Tech Giants Like Facebook, Amazon and Google be Broken Up?*, N.Y. TIMES (2019), https://www.nytimes.com/interactive/2019/us/politics/big-tech-democratic-candidates.html [https://perma.cc/P5LT-PEZH].

257. CAL. CIV. CODE § 1798.120 (West 2020).

258. Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (1st Sess. 2019).

259. *Id.* § 6.