Berkeley Technology Law Journal

Volume 29
Issue 1 *Spring*

Article 3

5-1-2014

Why Not Privacy by Default?

Lauren E. Willis

Link to publisher version (DOI)
http://dx.doi.org/https://doi.org/10.15779/Z38X40V

WHY NOT PRIVACY BY DEFAULT?

Lauren E. Willis[†]

ABSTRACT

We live in a Track-Me world, one from which opting out is often not possible. Firms collect reams of data about all of us, quietly tracking our mobile devices, our web surfing, and our email for marketing, pricing, product development, and other purposes. Most consumers both oppose tracking and want many of the benefits tracking can provide. In response, policymakers have proposed to give consumers significant control over when, how, and by whom they are tracked through a system of defaults (i.e., "Track-Me" or "Don't-Track-Me") from which consumers can opt out.

The use of a default scheme is premised on three assumptions. First, that for consumers with weak or conflicted preferences, any default chosen will be "sticky," meaning that more consumers will stay in the default position than would choose it if reaching the position required an affirmative action. Second, that those consumers with a true preference for the opt-out position—and only those consumers—will opt out. Third, that where firms oppose the default position, convincing consumers to opt out will require the firms to explain the default position, resulting in well-informed decisions by consumers.

This Article argues that for tracking defaults, these assumptions may not consistently hold. Past experience with the use of defaults in policymaking teaches that Track-Me defaults are likely to be too sticky, Don't-Track-Me defaults are likely to be too slippery, and neither are likely to result in well-educated consumers.

These conclusions should inform the "Do-Not-Track" policy discussions now taking place in the United States, in the European Union, and at the World Wide Web Consortium. They also cast doubt on the privacy and behavioral economics literatures that advocate the use of "nudges" to improve consumer decisions about privacy.

---

† Robert S. Braucher Visiting Professor of Law, Harvard Law School and Professor of Law, Loyola Law School Los Angeles, lauren.willis@lls.edu. My thanks to Omri Ben-Shahar, James Grimmelmann, Chris Hoofnagle, Paul Ohm, Jules Polonetsky, Paul Schwartz, Chris Soghoian, Lior Strahilevitz, Jessamyn West, Jonathan Zittrain, participants at the 2013 Privacy Law Scholars Conference, research assistant Natalie Kim, and the patient editors at the *Berkeley Technology Law Journal*.

TABLE OF CONTENTS

I. **INTRODUCTION** 64

II. **WHY AND WHEN DEFAULTS ARE STICKY** 69

A. MECHANISMS THAT MAKE DEFAULTS STICKY 72
1. *Transaction Barriers* 72
2. *Judgment and Decision Biases* 74
3. *Preference-Formation Effects* 77
B. CONDITIONS UNDER WHICH DEFAULTS ARE OFTEN STICKY 78

III. **DEFAULTS IN THEORY** 80

A. THE THEORY BEHIND THE USE OF DEFAULTS IN POLICYMAKING 80
1. *Policy Defaults* 81
2. *Penalty Defaults* 82
3. *Altering and Framing Rules* 82
4. *An Aside on Forced Choice* 84
B. TRANSLATING DEFAULT THEORY TO TRACKING POLICY 85
1. *Scope of Tracking Defaults* 86
2. *Setting: Track-Me or Don't-Track-Me* 88
3. *Granularity of Available Opt-Out Positions* 90
4. *Altering and Framing Rules* 92

IV. **DEFAULTS IN PRACTICE** 95

A. TWO FAILED DEFAULT SCHEMES 96
1. *The Financial Information Default Scheme* 96
2. *The Checking Account Overdraft Default Scheme* 97
B. HOW FIRMS MAKE THESE DEFAULTS FAIL 99
1. *Transaction Barriers* 99
2. *Judgment and Decision Biases* 102
3. *Preference Formation Effects* 105
C. SUCCESSFUL DEFAULTS 107
1. *Automatic Enrollment in Retirement Savings Plans* 107
2. *Do Not Call* 108
D. CRACKS IN THE THEORY BEHIND THE USE OF DEFAULTS 109
1. *Conditions Where Defaults Do Not Work* 109
2. *Reexamining the Logic Supporting the Use of Defaults in Policymaking* 110

V. **WHY TRACKING DEFAULTS ARE UNLIKELY TO ACHIEVE POLICYMAKERS' GOALS** 111

A. HOW FIRMS COULD MAKE TRACKING DEFAULTS FAIL 112
1. *Erect, Eliminate, or Invert Transaction Barriers* 112

a) Costs 112
b) Confusion 114
c) Futility 114
2. *Harness Judgment and Decision Biases* 115
a) Salience effects 115
b) Omission Bias 116
c) Loss Aversion and the Endowment Effect 116
d) Procrastination and Decision Avoidance 117
e) Excessive Discounting 117
f) Choice Bracketing 118
g) The Illusion of Control 118
h) The Sunk Costs Fallacy 119
3. *Bolster, Undermine, or Reverse Preference Formation Effects* 120
a) The Endorsement Effect 120
b) The Experience Effect 120
B. ALTERING RULES, FRAMING RULES, AND COMPETITION 121
1. *The Limits of Altering and Framing Rules* 122
a) Respect for Heterogeneous Preferences 122
b) Mis-sorting 124
c) Commercial Speech Doctrine Limits 125
d) The First and Last Mover 126
2. *Will Competition Change the Calculus?* 128
VI. **CONSEQUENCES OF PRIVACY POLICY BY DEFAULT** 130

I. INTRODUCTION

We live in a Track-Me[1] world, one from which opting out is, as a practical matter, often not possible. Firms collect reams of data about us for marketing, pricing, product development, and other uses. Sometimes we knowingly participate in the first stage of this process—a firm asks for information, and we provide it, knowing roughly how that firm will use it. But much data collection is passive, invisible, and performed without explicit consent. Most of us know little about downstream users to whom our data may be transferred and none of us can know all the future uses to which our data may be put. Collection of data on the websites we visit, the content of our emails, and the movements of our mobile phones have garnered the most media attention,[2] but as tracking technologies (e.g., facial recognition programs, eye tracking systems, and geolocation sensors) become cheaper and more accurate, the amount of data collected passively and the uses to which it will be put will only increase.[3]

Although preferences for information privacy vary, wide majorities of people both express opposition to the extent of this data collection and have taken some steps to avoid being tracked.[4] They wish to avoid uses of their

1. This Article uses "Track-Me" and "Don't-Track-Me" to avoid the indeterminacy of "Opt-In" and "Opt-Out," and uses "tracking" in a colloquial sense to refer to all forms of personal data collection and use for commercial purposes, online and off. For a discussion of "Do-Not-Track" as a technical protocol, see DO NOT TRACK—UNIVERSAL WEB TRACKING OPT OUT, http://donottrack.us (last visited Aug. 1, 2013). Collection and use of personal data for law enforcement purposes is beyond the scope of this Article.

2. Most websites track users, collecting information such as access time, visit duration, mouse movements, and clicks. *See* Andrew Couts, *Top 100 Websites: How They Track Your Every Move Online*, DIGITAL TRENDS (Aug. 30, 2012), http://www.digitaltrends.com/web/top-100-websites-how-are-they-tracking-you (finding that the top 100 websites all track users in some way). Some providers of "free" email scan users' email text. *See, e.g.*, John Pallatto, *Google Defends Scanning E-Mail for Ad Links*, EWEEK (Apr. 23, 2004), http://www.eweek.com/c/a/Messaging-and-Collaboration/Google-Defends-Scanning-EMail-for-Ad-Links (explaining that Google scans email text of Gmail users for targeted ad purposes). Mobile data is often tracked through applications or by cell carriers themselves, then sold to third parties. *See, e.g.*, Olga Kharif & Scott Moritz, *Cell Carriers Sell Users' Tracking Data in $5.5 B Market*, DELAWAREONLINE (June 13, 2013), http://www.delawareonline.com/article/20130613/BUSINESS08/306130050/Cell-carriers-sell-users-tracking-data-5-5-B-market (reporting on multi-billion dollar market for cell phone tracking data).

3. *See generally What They Know*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Aug. 1, 2013) (providing an overview of current news and issues regarding Internet tracking).

4. *See, e.g.*, LEE RAINIE ET AL., ANONYMITY, PRIVACY, AND SECURITY ONLINE, PEWRESEARCHCENTER REP. 8 (Sept. 5, 2013), http://pewinternet.org/~/media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf (finding that eighty-six percent of internet users have "taken at least one step to try to mask their behavior or avoid being

data that they experience as harmful (e.g., identity theft, price discrimination, negative employment consequences) as well as the more amorphous costs of a lack of privacy (e.g., the "creepy" feeling of being watched, personal embarrassment and social stigma, decreased space for individual experimentation and reflection).[5] Yet, people want the benefits that tracking can provide, such as online socializing and access to online content.[6]

In response, policymakers have proposed that firms provide consumers with significant control over when, how, and by whom they are tracked through a system of defaults (i.e., "Track-Me" or "Don't-Track-Me") from which consumers can opt out.[7] Ostensibly, this "notice and choice" regime is motivated by a desire to satisfy heterogeneous privacy preferences. Such an approach has deep normative roots; privacy itself has been conceptualized as a right of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others."[8] Defaults as privacy policy also relieve policymakers of some of the contested judgment

tracked"); Chris Crum, Googler: Nobody Wants to Be Tracked Online, WEBPRONEWS (Apr. 2, 2012), http://www.webpronews.com/googler-nobody-wants-to-be-tracked-online-2012-04 (finding that nearly eighty-five percent of users think a business should not be able to anonymously track consumer activity on the business's website).

5. *See, e.g.*, Mark Memmott, *Orbitz Shows Mac Users Pricier Hotel Options: Big Deal or No Brainer?*, THE TWO-WAY: BREAKING NEWS FROM NPR (June 26, 2012), http://www.npr.org/blogs/thetwo-way/2012/06/26/155756095/orbitz-shows-mac-users-pricier-hotel-options-big-deal-or-no-brainer (showing that 85% of readers said they "[w]ould . . . be upset to learn [they] had been shown pricier options just because [they] used a Mac to search for a hotel"); ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011) (arguing that privacy is often necessary for personal dignity, trust, and reputation, all of which preserve freedom to make one's own social, economic, and political choices).

6. *See, e.g.*, Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 64 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf (listing significant benefits currently produced by tracking).

7. *See, e.g.*, Do-Not-Track Online Act of 2013, S. 418, 113th Cong. (2013) (proposing legislation that would require the FTC to create an enforceable "mechanism by which an individual can simply and easily indicate whether the individual prefers to have personal information collected by providers of online services, including by providers of mobile applications and services"); THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 11–22 (2012) (proposing a Consumer Privacy Bill of Rights, which includes: "Consumers have a right to exercise control over what personal data companies collect from them and how they use it.").

8. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). This focus on individual choice may be misplaced, regardless of whether meaningful choice is possible. Social welfare and individual preferences about privacy may not be well aligned, and if so, policymakers ought to make policy based on the social costs and benefits of tracking rather than based on a quest to satisfy preferences. But that debate is beyond the scope of this Article.

calls presented by the social costs and benefits of tracking, leaving each consumer to make an individual cost-benefit tradeoff for herself.[9]

The use of a default scheme from which consumers can opt out is premised on three key assumptions, taken from behavioral economics literature.[10] First, that any default will be "sticky," meaning that more consumers stay with the default than would explicitly choose to do so if forced to make a choice.[11] Second, that those consumers with a true preference for the opt-out position—and only those consumers—will opt out.[12] Third, that where a firm opposes the default position, the firm will be forced to explain it in the course of trying to convince consumers to opt out, resulting in well-informed decisions by consumers.[13] In behavioral economics

9. *Cf.* JAMES P. NEHF, OPEN BOOK: THE FAILED PROMISE OF INFORMATION PRIVACY IN AMERICA 103–04 (2012) (explaining difficulty policymakers have with resolving the incommensurability of the costs and benefits of privacy).

10. A fourth key assumption is that defaults imposed by law can and will be enforced. These assumptions may be naive, as experiences in the European Union, in Israel, and with the Children's Online Privacy Protection Act ("COPPA") in the United States, suggest. *See, e.g.*, Maurizio Borghi et al., *Online Data Processing Consent Under EU Law: A Theoretical Framework and Empirical Evidence from the UK*, 21 INT'L. J. L. & INFO. TECH. 109 (2013) (finding widespread noncompliance with E.U. and U.K. law requiring user consent prior to data collection); Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOMM. & TECH. L. REV. 337 (2011) (finding widespread noncompliance with Israeli law requiring notice to users about data collection); EUROPEAN NETWORK AND INFO. SEC. AGENCY, PRIVACY CONSIDERATIONS OF ONLINE BEHAVIOURAL TRACKING 16 (2012), http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking (finding that EU law requiring user consent prior to tracking is not being enforced by the EU or member countries); danah boyd et al., *Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act*,*'* 16 FIRST MONDAY 11 (2011), http://firstmonday.org/ojs/index.php/fm/article/view/3850/3075 (finding widespread circumvention of COPPA's default that websites cannot collect information about children unless their parents opt out). To present the strongest case for tracking defaults, this Article assumes they would be enforceable and enforced, but nonetheless finds that tracking defaults are unlikely to achieve policymakers' professed aims.

11. *See, e.g.*, Cass R. Sunstein, Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych 9 (May 19, 2013) (unpublished manuscript), *available at* http://ssrn.com/abstract_id=2171343 ("In the domain of privacy on the Internet, a great deal depends on the default rule.").

12. *See, e.g.*, Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 633 (2006) (suggesting penalty defaults for privacy settings to protect uninformed users yet allow "well-informed individuals" to opt out).

13. *See, e.g.*, Lilian Edwards & Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION 202, 225 (A. Matwyshyn ed., 2009) ("A general rule that privacy settings be set at the most privacy-friendly setting when a profile is first set up . . . would inform all users that privacy

parlance, tracking defaults are expected to be sticky "policy defaults" (intended to nudge people with weak or unformed preferences toward the default position)[14] or information-forcing "penalty defaults" (intended to educate people about the default and opt-out positions).[15]

This Article demonstrates one reason why tracking defaults will not necessarily nudge consumers to the right position or help consumers meet their own well-informed preferences: the assumptions underlying the use of defaults in policymaking are unlikely to hold in the personal-data-tracking context. Defaults can be too sticky (meaning that consumers stick with the default even though they would opt out were they well-informed) or too slippery (meaning that consumers opt out even though they would prefer the default position were they well-informed), and defaults are not always information-forcing. Firms surround defaults they favor with a powerful campaign to keep consumers in the default position, but meet defaults set contrary to their interests with an equally powerful campaign to drive consumers to opt out. Rather than giving firms an incentive to facilitate consumer exercise of informed choice, many defaults leave firms with opportunities to play on consumer biases or confuse consumers into sticking with or opting out of the default.

Thus, whether a tracking default is sticky or slippery, informative or uninformative will depend on whether firms' interests are aligned with the default. To counter firm manipulation, the law can impose altering rules[16]—rules governing the process by which consumers can opt out—and framing rules[17]—rules governing the presentation of the default to consumers. But normative, legal, and practical constraints limit altering and framing rules, and even the strongest of such rules can be outmaneuvered by firms with the means and motivation to do so.

Unless robust competition over protecting consumer privacy develops in the marketplace—a doubtful prospect—firms will generally prefer for

settings do exist, and force them to learn how to make use of them before they moved on to networking . . . .").

14. *See, e.g.*, Craig R. M. McKenzie et al., *Recommendations Implicit in Policy Defaults*, 17 PSYCHOL. SCI. 414, 414–15 (2006) (defining "policy default" in the context of organ donation).

15. Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 91 (1989); *see also* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1239 (2001) (dubbing penalty defaults "information-forcing defaults").

16. *See* Ian Ayres, *Regulating Opting Out: An Economic Theory of Altering Rules*, 121 YALE L.J. 2032 (2012).

17. *See* Elizabeth F. Emens, *Changing Name Changing: Framing Rules and the Future of Marital Names*, 74 U. CHI. L. REV. 763, 840 (2007).

consumers to be in the Track-Me position. Because firms can influence people's responses to tracking defaults, most Track-Me defaults will be too sticky and many Don't-Track-Me defaults will be too slippery. Further, neither the consumers who remain in Track-Me defaults nor those who opt out of Don't-Track-Me defaults will necessarily be making well-informed decisions. Personal-data-tracking defaults, therefore, are unlikely to facilitate the satisfaction of heterogeneous consumer preferences or produce an informed resolution of the conflict between people's desire for information privacy and their desire for the benefits produced by their data.

Privacy law scholars have been skeptical of the idea that a notice-and-choice regime could produce robust individual decision making about personal data privacy.[18] Yet their critiques have not confronted, and have even equivocated in the face of, the assumptions about defaults made by the standard behavioral economics literature.[19] Some scholars continue to advocate defaults, but on norms-setting grounds rather than as policy defaults or penalty defaults.[20] For defaults to set these norms, however, the signals that defaults provide must be clear. Experiences with other default rules give reason to think that firms will surround tracking defaults with a great deal of noise—noise calculated to confuse the signal.

This Article fills the current intellectual gap with an understanding of how firms' dynamic responses to defaults can undermine policymakers' aims. It thus exposes the limits of defaults as policy tools. Along the way, this Article provides several new insights into defaults: that nearly any bias might lead a consumer to stay in a default position, not just those biases typically

18. The classic article on personal information tracking defaults is Janger & Schwartz, *supra* note 15. *See also, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1660–63, 1681–85 (1999) (critiquing the individual choice model of privacy); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013) (same).

19. *See, e.g.*, Schwartz, *supra* note 18, at 1686–87 (suggesting that a default of minimal data disclosure would allow individuals to "personalize their privacy levels"); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2100 (2004) ("This Article prefers an opt-in default because . . . it would place pressure on the better-informed party to disclose material information about how personal data will be used. This default promises to force the disclosure of hidden information about data-processing practices."); Solove, *supra* note 18, at 1900 ("[P]rivacy self-management should not be abandoned. . . .").

20. *See, e.g.*, Solove, *supra* note 18, at 1903 ("The law should develop and codify basic privacy norms . . . . [I]t can be in a form like the Uniform Commercial Code (UCC), where certain default rules can be waived."); 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, 341 (2012) (suggesting that tracking defaults be used to signal and effectively set social norms about what information should and should not be shared, with whom, and under what conditions).

associated with defaults; that the theory underlying the use of defaults in policymaking fails to address how policymakers should set the scope of defaults and the granularity of opt-out choices; and that the faith in the potential for altering and framing rules to fine-tune the stickiness of defaults is misplaced. Finally, this Article casts doubt on the use of "nudges"[21] in policymaking to help people make better choices about information privacy.[22] While Track-Me and Don't-Track-Me defaults might pave the political path to a better system for regulating personal data tracking, they might also defuse the political will to implement better privacy regulation.

This Article proceeds as follows: Part II describes why and when defaults are sticky. Part III explains the theory behind the use of defaults in policymaking and how policymakers appear poised to translate these theories to the personal-data-tracking arena. Part IV examines the use of defaults in other contexts to assess when and why defaults in practice do and do not function as theorized. Part V considers how tracking defaults can be expected to play out, predicting that Track-Me defaults are likely to be overly sticky and Don't-Track-Me defaults are likely to be overly slippery. Part V also explains why altering rules, framing rules, and competition have limited potential to change these dynamics. Part VI concludes with an exploration of the potential political consequences of using defaults in information privacy policy.

II. WHY AND WHEN DEFAULTS ARE STICKY

A default is a setting or position that has been preselected, but can be altered. For example, many email programs by default have an audible

21. *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008) (defining a "nudge" as a policy tool that "alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives").

22. A burgeoning literature advocates the use of nudges to encourage people to make better privacy decisions. *See, e.g.*, Rebecca Balebako et al., *Nudging Users Towards Privacy on Mobile Devices*, *in* PROCEEDINGS OF THE 2ND INTERNATIONAL WORKSHOP ON PERSUASION, INFLUENCE, NUDGE & COERCION THROUGH MOBILE DEVICES (2011); M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012); Yang Wang et al*., Privacy Nudges for Social Media: An Exploratory Facebook Study*, Second International Workshop on Privacy and Security in Online Social Media (2013), *available at* http://precog.iiitd.edu.in/events/psosm2013/9psosm6-wang.pdf; Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, 7 IEEE 82 (2009).

notification for incoming mail, but the user can turn off the notification or change the sound.[23]

Default settings by definition can be changed, yet few people change them. Tracking consumer activity on the Internet today presents a rough example. Many websites, mobile phones, applications ("apps"), and other devices and programs that can facilitate or inhibit tracking are preset to allow tracking today.[24] Many of these settings are not full-fledged defaults because opting out is not always possible; some devices and programs cannot be used without tracking enabled, and some trackers track consumers even when program or device settings are in the "Do-Not-Track" position.[25] But consumers can opt out of some tracking, at least partially, such that "Track-Me" is a quasi-default today. Consumers can delete certain types of cookies from their browsers or install software that blocks some Internet and cellphone tracking.[26] Consumers can also change tracking options on their

23. *See, e.g.*, *Customize Your AOL Sounds*, AOL HELP, http://help.aol.com/help/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=217059 (last visited Dec. 1, 2013).

24. *See, e.g.*, Claire Cain Miller, *How to Opt Out of Google's Plan to Use Your Name and Comments in Ads*, N.Y. TIMES (Oct. 14, 2013), http://bits.blogs.nytimes.com/2013/10/14/how-to-opt-out-of-googles-plan-to-use-your-name-and-comments-in-ads (discussing how some of Google's settings are set by default to Track-Me); Andrew Couts, *Are Apple's iOS 7 Privacy Settings Purposefully Misleading, or Just a Mess?,* DIGITAL TRENDS (Sept. 29, 2013), http://www.digitaltrends.com/mobile/apple-your-ios-7-privacy-settings-are-a-mess/#ixzz2iCafwri3 (discussing iPhone defaults set to enable tracking). Although most tracking settings are set by default to Track-Me, a few are not. *See, e.g.*, *Safari Blocks all Cookies by Default*, APPLE SUPPORT COMMUNITIES, https://discussions.apple.com/thread/4040376 (last visited Aug. 1, 2013).

25. *See, e.g.*, Peter Maass & Megha Rajagopalan, *That's No Phone. That's My Tracker*, PROPUBLICA (July 13, 2012), http://www.propublica.org/article/thats-no-phone.-thats-my-tracker (reporting that cellphone tracking may continue even if phone is powered down); *Google: Gmail Users 'Have No Legitimate Expectation of Privacy,'* RT.COM (Aug. 13, 2013), http://on.rt.com/47y0ku (reporting that Gmail cannot be used without allowing Google to scan email content for various purposes); Katy Bachman, *Yahoo Says No to Microsoft's 'Do Not Track' Browser, Others Expected to Follow Suit*, ADWEEK (Oct. 26, 2012), http://www.adweek.com/news/technology/yahoo-says-no-microsofts-do-not-track-browser-144847 (reporting that Yahoo and others will not honor a "Do-Not-Track" signal received from an Internet Explorer browser). *See generally* Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. J.L. & PUB. POL'Y 273 (2012) (detailing how trackers have evaded technology consumers use to prevent tracking).

26. *See, e.g.*, Alan Henry, *Everyone's Trying to Track What You Do on the Web: Here's How to Stop Them*, LIFEHACKER (Feb. 22, 2012), http://lifehacker.com/5887140/everyones-trying-to-track-what-you-do-on-the-web-heres-how-to-stop-them; Erica Naone, *Smartphone Apps: How to Spot and Stop Firms Tracking Your Phone*, CHRISTIAN SCIENCE MONITOR (May 5, 2011), http://www.csmonitor.com/Innovation/Latest-News-Wires/2011/0505/Smartphone-apps-How-to-spot-and-stop-firms-tracking-your-phone.

Facebook, Twitter, or Google accounts,[27] and they can set their browsers to ask websites not to track them.[28]

While a majority of consumers claim they have taken at least some steps to opt out of Internet tracking,[29] these claims are surely more aspirational than representational.[30] It is extremely unlikely that many consumers successfully opt out on each device, browser, and app through which they are tracked. Currently, about 17% of Firefox users in the United States have their browsers set to "Do Not Track."[31] Fewer than 10% of consumers even know that common mobile phone apps track them.[32] Firms that claim they can track nearly all Americans across all their devices may be exaggerating, but probably not by much.[33] Despite widespread opposition to tracking, most consumers stick with most preset Track-Me positions.

---

27. *See, e.g.*, Alan Henry, *Facebook Is Tracking Your Every Move on the Web; Here's How to Stop It*, LIFEHACKER (Sept. 26, 2011), http://lifehacker.com/5843969/facebook-is-tracking-your-every-move-on-the-web-heres-how-to-stop-it; Ryan Tate, *How Google Spies on Your Gmail Account (And How To Stop It)*, GAWKER (May 11, 2011), http://gawker.com/5800868/how-google-spies-on-your-gmail-account-and-how-to-stop-it; Alan Henry, *Twitter Wants to Start Tracking You on the Web, Here's How to Opt-Out*, LIFEHACKER (July 3, 2013), http://lifehacker.com/twitter-wants-to-start-tracking-you-on-the-web-heres-661569459.

28. *See, e.g.*, Thorin Klosowski, *Everywhere You Can Enable 'Do Not Track*,*'* LIFEHACKER (Aug. 5, 2013), http://lifehacker.com/everywhere-you-can-enable-do-not-track-1006138985.

29. *See* Rainie et al., *supra* note 4, at 8 (finding that eighty-six percent of consumers claim to have taken at least one step to avoid being tracked).

30. Consumers claim to engage in significantly more privacy-protective online behavior than they truly do. *See* Carlos Jensen et al., *Privacy Practices of Internet Users: Self-reports Versus Observed Behavior*, 63 INT. J. HUMAN-COMPUTER STUD. 203, 226 (2005).

31. Alex Fowler, *Mozilla's New Do Not Track Dashboard: Firefox Users Continue to Seek out and Enable DNT*, MOZILLA PRIVACY BLOG (May 3, 2013), https://blog.mozilla.org/privacy/2013/05/03/mozillas-new-do-not-track-dashboard-firefox-users-continue-to-seek-out-and-enable-dnt.

32. David Talbot, *Using Crowdsourcing to Protect Your Privacy*, MIT TECH. REV. (Apr. 2, 2012), http://www.technologyreview.com/news/427390/using-crowdsourcing-to-protect-your-privacy.

33. While consumers claim to engage in privacy-protective behavior, firms that collect personal data advertise that they have extensive data on most U.S. adults. *See* Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 16, 2012, *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html. One firm claims that it can use digital fingerprinting technology, a technology that does not depend on cookies and can identify both mobile devices and computers, to identify ninety-eight percent of Internet users. *See* Adam Tanner, *The Web Cookie Is Dying. Here's the Creepier Technology That Comes Next*, FORBES, June 17, 2013, http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/. Another firm claims its technology can match 1.5 billion devices and that "its pinpointing [is] so accurate that it c[an] show spouses different, personalized ads on a tablet they share." Claire Cain Miller & Somini Sengupta, *Selling Secrets*

Why do people adhere to default settings even when they dislike those settings? The following Section surveys the mechanisms that make defaults sticky and the conditions under which these mechanisms operate.

A. MECHANISMS THAT MAKE DEFAULTS STICKY

Three types of mechanisms can operate to make defaults sticky: (a) transaction barriers, (b) judgment and decision biases, and (c) the preference-forming effects of defaults.[34] Not every mechanism will affect every default, but where a default is sticky, one or more of these mechanisms are at work.

1. Transaction Barriers

Transaction barriers include the costs of opting out, confusion about the default setting or the opt-out process, and a sense of futility where opting out seems to be impossible. Today's Track-Me quasi-default provides an example of all of these factors.

Opting out of tracking today is costly. Consumers must find the opt-out procedure, if one exists, and execute the steps for opting out, such as installing a program, changing settings, or completing an online form. Even when opting out of a single Track-Me setting is not onerous, it must be completed for each device (e.g., cellphone, tablet, desktop) and program through which one can be tracked.[35] If a consumer wants to indicate fine-grained preferences, the number of firms from which the consumer would need to opt out—on each browser on each device the consumer uses—is vast. One reporter counted over 100 companies that tracked him online in a thirty-six-hour period of ordinary web use.[36] Further, some of these steps must be repeated when consumers upgrade devices or software.[37] In addition, if a consumer deletes all cookies, cookies that had been sending "Do-Not-Track" messages must be reinstalled.[38]

---

of Phone Users to Advertisers, N.Y. TIMES, Oct. 5, 2013, *available at* http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html.

34. For a more detailed explanation of some of the mechanisms that can make defaults sticky, see Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155 (2013).

35. *See, e.g.*, *Privacy Policy*, COX DIGITAL SOLUTIONS, http://www.coxdigitalsolutions.com/privacy_policy.html (last visited Apr. 11, 2014) ("If you use more than one type of browser or more than one computer to access the Internet, you will have to opt out in each browser and on each computer that you use.").

36. Alexis Madrigal, *Digital Shadow: How Companies Track You Online*, WEEK (Apr. 13, 2012), http://theweek.com/article/index/226708/digital-shadow-how-companies-track-you-online.

37. *See, e.g.*, *Privacy Policy*, *supra* note 35 ("You may need to opt out repeatedly. If you delete or otherwise alter your browser's cookie file (including upgrading certain browsers) you may need to opt out again.").

38. *Id.*

Further, several misconceptions about tracking deter opting out. Many people do not even know that firms today can track their Internet use, scan their email text, and follow their device movements for commercial purposes.[39] In one survey nearly all respondents were surprised that a popular flashlight app sent the user's unique cellphone ID and precise location to advertisers.[40] Most consumers falsely believe that the law significantly restricts collection of consumer information[41] and that the existence of a "Privacy Policy" means their information is not shared with third parties.[42] Mistaken about what happens if they do nothing, consumers who prefer not to be tracked have no reason to opt out. Other consumers know about tracking but are unaware of the (albeit limited) ways in which they can opt out.[43] Invisibility of the option to opt out inevitably leads to sticking with the default. Finally, many consumers think they know more about technology related to privacy than they do.[44] Popular misconceptions include the belief that changing browser settings or deleting cookies disables Internet tracking.[45] The result is that consumers who attempt to opt out of tracking

39. *See, e.g.*, Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities That Enable It* 21, tbl.9 (Sept. 29, 2009) (unpublished manuscript), *available at* http://ssrn.com/abstract=1478214 (finding that only thirty-three percent of users in 2009 survey knew that their Internet use could be tracked across multiple websites without their consent); Adario Strange, *Google's Snooping Gmail the Target of Microsoft's Latest 'Scroogle' Attack*, ITPROPORTAL (Feb. 8, 2013), http://www.itproportal.com/2013/02/08/googles-snooping-gmail-the-target-of-microsoft-latest-scroogle-campaign (reporting that fewer than thirty percent of Gmail users surveyed knew that their email text was scanned for behavioral advertising purposes); Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES, July 14, 2013, http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html (reporting that shoppers were surprised that their movements within a store were monitored through their cellphones).

40. Talbot, *supra* note 32.

41. *See* Turow et al., *supra* note 39, at 21, tbl.9 (2009).

42. Jensen et al., *supra* note 30, at 223; *see also* Ilana Westerman, *What Misconceptions Do Consumers Have About Privacy?*, PRIVACY PERSPECTIVES (June 3, 2013), https://www.privacyassociation.org/privacy_perspectives/post/what_misconceptions_do_consumers_have_about_privacy (discussing the misconceptions consumers have about privacy generally).

43. Two-thirds of consumers are unaware of options they have to limit how much information is collected about them. *See* KRISTEN PURCELL ET AL., SEARCH ENGINE USE 2012, PEW INTERNET & AMERICAN LIFE PROJECT 3 (2012); *see also* Annalect Research Group, *Internet Users' Response to Consumer Online Privacy*, ANNALECT.COM (Mar. 14, 2012), http://annalect.com/white-paper-internet-users-response-to-consumer-online-privacy (finding only twenty-two percent of users aware of some ability to opt out of tracking).

44. *See* Jensen et al., *supra* note 30, at 226.

45. Hoofnagle et al., *supra* note 25, at 277 (changing browser settings or deleting cookies does not prevent all tracking).

today often do not manage to do so to the extent they desire or even mistakenly believe they have done.[46]

A sense of futility presents another barrier to opting out.[47] Some consumers understand that the Track-Me position today is a quasi-default, not a true default, in that entirely opting out is not possible.[48] Others, perhaps accurately given the confusion associated with opting out, believe that they lack the expertise necessary to successfully opt out.[49] Rather than engage in futile attempts to opt out of the default, these consumers might not even try.[50]

2. Judgment and Decision Biases

Judgment and decision biases are another type of mechanism through which defaults can attract adherents. One pair of such biases that can pull people towards a default position is loss aversion[51] and the endowment effect.[52] Experiments in the personal-data-tracking arena illustrate the way in

46. Pedro G. Leon et al., *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, *in* CHI 2012, ACM Press 589–98 (2012), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf ("[M]ultiple participants opted out of only one company . . . despite intending to opt out of all. Others mistook the [registration] page . . . as the opt out page."); *see also* Janger & Schwartz, *supra* note 15, at 1241 (noting that confusing and misleading privacy notices are designed to lead to consumer inaction).

47. *Cf.* Chad A. Proell & Stephen Sauer, *"Stock" Options: The Debilitating Effects of Autonomy and Choice on Self-perceptions of Power*, 23 J. OF BUS. & BEHAV. SCI. 82 (2011) (describing how feelings of powerlessness lead to inaction).

48. Rainie, *supra* note 4, at 12.

49. *See, e.g.*, Blasé Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising* 8–9 (Carnegie Mellon Univ., Working Paper No. CMU-CyLab-12-007, 2012), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12007.pdf (reporting that in response to questions about opting out of behavioral advertising, many consumers expressed uncertainty about how to opt out); *Yet Another OPT OUT You Should Think About*, BOXLOUR MEDIA (Oct. 20, 2013), http://www.boxlour.com/?p=319 ("Typically the process to opt out of something is not as easy as a 'click here' button. In fact, they are literally banking on most of us getting so confused on the whole 'opt out' process that we eventually give up. And give up we do.").

50. *See, e.g.*, Blasé Ur et al., *supra* note 49, at 7 (quoting consumer: "It makes me want to go home and delete all my cookies, but then I know that's not gonna help much."); Maria Karyda & Spyros Kokolakis, *Privacy Perceptions Among Members of Online Communities*, *in* DIGITAL PRIVACY 253, 263 (Alessandro Acquisti et al. eds., 2010) (discussing consumer sentiments that user attempts to obtain privacy on the Internet are futile).

51. Loss aversion means weighing losses more heavily than gains against some reference point. *See, e.g.*, William Samuelson & Richard Zeckhauser, *Status Quo Bias in Decision Making*, 1 J. RISK & UNCERTAINTY 7, 19, 31 (1988).

52. The endowment effect, placing a higher value on what one already possesses (or perceives oneself as possessing) than on the same thing when one does not possess it, is a manifestation of loss aversion. *See, e.g.*, Russell Korobkin, *Wrestling with the Endowment Effect,*

which these biases can favor a default position. This research demonstrates an almost absurdly strong endowment effect for privacy. On average, people will give up much more to keep data private when it is private by default, compared to what they will pay to obtain privacy when told the default is for that data to be public; subjects in one experiment "were five times more likely to reject cash offers for their data if they believed that their privacy would be, by default, protected, than if they didn't enjoy such belief."[53] Because today's default is for data not to be private, these biases favor the Track-Me position.

In addition to loss aversion and the endowment effect, the biases that have been identified in the existing literature as contributing to the magnetism of defaults include salience effects,[54] omission bias,[55] and procrastination and decision avoidance.[56] But the existing literature fails to recognize that nearly *any* type of bias might be invoked to favor a default, provided the necessary conditions exist to facilitate the operation of biases. In the case of tracking, for example, excessive discounting,[57] choice

or How to Do Law and Economics Without the Coase Theorem 16 (UCLA Sch. of Law, Law-Econ Research Paper, Paper No. 13-10, 2013), *available at* http://ssrn.com/abstract_id=2289574.

53. *See* Alessandro Acquisti et al., *What Is Privacy Worth* 3, *in* 21ST WORKSHOP ON INFORMATION SYSTEMS AND ECONOMICS (2009), *available at* http://www.futureofprivacy.org/wp-content/uploads/2010/07/privacy-worth-acquisti-FPF.pdf. Similar results were obtained in Jens Grossklags & Alessandro Acquisti, *When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, Workshop on the Economics of Information Security (2007), *available at* http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags_Acquisti-WEIS07.pdf.

54. The salience effect is the tendency for salient information to disproportionately affect judgments and non-salient information to be ignored. *See, e.g.*, Tanjim Hossain & John Morgan, . . . *Plus Shipping and Handling: Revenue (Non) Equivalence in Field Experiments on eBay*, 62 ADVANCES IN ECON. ANALYSIS & POL'Y 1, 20 (2006).

55. Omission bias is the tendency to favor inaction over action. It is believed to be caused by a desire to avoid future regret and the fact that people more commonly blame themselves about a poor outcome when they take action than when they fail to take action. *See, e.g.*, Jonathan Baron & Ilana Ritov, *Reference Points and Omission Bias*, 59 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 475, 478 (1994).

56. Procrastination and decision avoidance are biases triggered when decisions or actions appear difficult. These biases can cause people to procrastinate indefinitely or affirmatively decide not to make any decision, either of which could lead to sticking with the default. *See, e.g.*, Ted O'Donoghue & Matthew Rabin, *Choice and Procrastination*, 116 Q.J. ECON. 121 *passim* (2001); Christopher J. Anderson, *The Psychology of Doing Nothing: Forms of Decision Avoidance Result from Reason and Emotion*, 129 PSYCHOL. BULL. 139 *passim* (2003).

57. Excessive discounting refers to people's tendency both to prefer a much smaller gain now to a larger gain later and to prefer a sure gain to an uncertain but probabilistically much larger gain. *See, e.g.*, Yaacov Trope & Nira Liberman, *Construal-Level Theory of Psychological Distance*, 117 PSYCHOL. REV. 440 *passim* (2010) (explaining the tendency for people to discount over psychological distance, including over time and over uncertainty).

bracketing, the illusion of control,[58] and the sunk costs fallacy[59] all may draw consumers to today's Track-Me quasi-default.

Choice bracketing's effect on consumers facing a default may be particularly strong. Choice bracketing refers to whether a decision is evaluated in isolation or as part of a larger set of decisions.[60] Health-related decisions present an intuitive example. If the choice to eat a dessert or go for a run is made in isolation, the benefits of the dessert and costs of the run might easily outweigh the trivial effect of each on health. Yet, the cumulative effect of these daily decisions can be enormous. Someone who views each choice in isolation might make less healthy choices than someone who mentally brackets decisions about diet, exercise, or health broadly.[61]

Personal data privacy decisions present a similar structure. Tracking decisions can be conceived narrowly or broadly. One consumer might make each decision in isolation, considering whether to permit a particular entity to track her at a particular moment in time. Another consumer might conceptualize each tracking decision as part of a broader choice about whether to allow herself to be tracked by any entity anytime. Firms are able to connect data gathered from a variety of sources—off-line, online, and from mobile devices—about a single consumer, collected over time.[62] Thus,

58. The illusion of control is a bias that can lead people to take on more risk than they otherwise would, which might encourage consumers to stick with a risky default if surrounding circumstances invoke the illusion. *See, e.g.*, Mark S. Horswill & Frank P. McKenna, *The Effect of Perceived Control on Risk Taking*, 29 J. APPLIED SOC. PSYCHOL. 377 (1999); Ellen J. Langer, *The Illusion of Control*, 32 J. PERSONALITY & SOC. PSYCHOL. 311 (1975). An example of the illusion is the common belief that one is less prone to experience an accident when one is driving than when one is a passenger, regardless of driving skill. *See* Frank P. McKenna, *It Won't Happen to Me: Unrealistic Optimism or Illusion of Control?*, 84 BRIT. J. PSYCHOL. 39, 39–50 (1993).

59. The sunk costs fallacy refers to the common error of weighing irreversibly incurred costs in a decision about whether to continue with a project or switch course. Hal R. Arkes & Catherine Blumer, *The Psychology of Sunk Cost*, 35 ORG. BEHAV. & HUM. DECISION PROCESSES 124 (1985). For example, someone who has learned how to use one type of software might continue to use that software instead of switching to an easier-to-use program because otherwise the effort of learning the first software seems to have been wasted. But, because that time and effort can never be recovered, it should not come into the calculus about what software to use going forward. Where the option to opt out of a default is not presented until after people have invested in the default, the sunk costs fallacy will favor the default.

60. Daniel Read et al., *Choice Bracketing*, 19 J. OF RISK & UNCERTAINTY 171, 172 (2000).

61. *Cf. id.* at 171 (using example of decisions about smoking cigarettes).

62. *See, e.g.*, Somini Sengupta, *What You Didn't Post, Facebook May Still Know*, N.Y. TIMES, Mar. 25, 2013, *available at* http://www.nytimes.com/2013/03/26/technology/facebook-expands-targeted-advertising-through-outside-data-sources.html (describing aggregation of online and off-line data about individual consumers).

the benefits of privacy and costs of a lack of privacy depend on the whole of privacy, not its parts; it is impossible to know whether tracking by any particular party or of any particular piece of information will tip the scales.[63] Because the probable negative impact of tracking by any one tracker is negligible, bracketing the choice narrowly could incline consumers to allow tracking. In contrast, broad choice bracketing is more likely to lead consumers to select a Don't-Track-Me position because the entirety of potential harms from tracking looms larger.

People often accept the bracketing implicit in a decision's presentation,[64] and many tracking decisions today are presented in a narrow form—e.g., Would you like to opt out of "tailor[ed] ads" from Twitter?[65] Rather than presenting the user with a broad opt-out choice, a single device or program often requires opting out of a series of particular types of tracking.[66] Even where broader choices are presented, such as in browser settings, trackers can ask consumers to alter that setting as to a particular website, a narrow choice. Thus, narrow choice bracketing may fortify today's Track-Me position.

3. Preference-Formation Effects

In addition to transaction barriers and judgment and decision biases, the process of forming preferences can encourage people to keep default settings.[67] This happens in two ways, through the endorsement effect and the experience effect.

The endorsement effect is the interpretation of a default as a form of implicit advice by a more knowledgeable party as to what most people prefer or ought to prefer.[68] Often, consumers follow this implicit advice.[69] For example, when consumers believe tracking defaults are selected based on majoritarian preferences, they may accept them on that basis alone because when it comes to privacy, consumers are particularly prone to following the

63. *Cf.* Solove, *supra* note 18, at 1889–90 (dubbing this the "aggregation effect").

64. Read et al., *supra* note 60, at 188 ("[When] choices come to [people] one at a time, they will bracket them narrowly, and if choices come to them collectively, they will bracket more broadly.").

65. *See* Henry, *supra* note 27.

66. *See, e.g.*, Jason D. O'Grady, *Four Privacy Settings You Should Enable in iOS 7 Immediately*, ZDNET (Sept. 19, 2013), http://www.zdnet.com/four-privacy-settings-you-should-enable-in-ios-7-immediately-7000020902.

67. *See, e.g.*, Cass Sunstein, *Switching the Default Rule*, 77 N.Y.U. L. REV. 106 (2002) (discussing preference-formation effects of defaults).

68. *See, e.g.*, Eric J. Johnson & Daniel G. Goldstein, *Decisions by Default*, *in* THE BEHAVIORAL FOUNDATIONS OF PUBLIC POLICY 417, 421 (Eldar Shafir ed., 2013).

69. *See, e.g.*, McKenzie et al., *supra* note 14, at 414.

crowd.[70] Along the same lines, consumers may agree to today's Track-Me quasi-default because they trust the firms with which they do business and assume these firms have set the default with consumers' best interests in mind.[71]

The experience effect can lead people to develop a preference for the default position after spending some time experiencing it. For example, cellphone users who perceive themselves as benefitting from their existing privacy settings might choose to stick with a phone's Track-Me position. Yet, if Don't-Track-Me had been the phone's default setting, they would have become accustomed to that position and developed a preference for it instead.[72]

B. CONDITIONS UNDER WHICH DEFAULTS ARE OFTEN STICKY

The mechanisms that can give defaults traction do not operate consistently across all consumers, but rather vary with consumers' understanding of their options and of their own preferences. When consumers understand their options and their preferences well, they can usually match the two easily, absent transaction barriers. A consumer who knows she prefers the opt-out position will not be swayed by the implicit advice conveyed in the policymaker's selection of the default, for example.[73] Likewise, consumers who already know their options are less affected by how salient each option is at the moment of decision. In these situations, biases and the preference-formation effects of defaults have little influence on outcomes. That is, defaults will not be sticky.[74]

---

70. Alessandro Acquisti et al., *The Impact of Relative Judgments on Concern About Privacy*, 49 J. MARKETING. RES. 3 (2012).

71. Although cellphone companies do not fare as well, Amazon, Google, and Apple are among the ten companies with the highest reputations among consumers, and trust is one of the major drivers of these ratings. HARRIS INTERACTIVE, THE HARRIS POLL 2013 RQ SUMMARY REPORT 6, 9 (2013), http://www.harrisinteractive.com/vault/2013%20RQ%20Summary%20Report%20FINAL.pdf.

72. *Cf.* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010 (2013) (suggesting that reactive nature of U.S. privacy policymaking leads to less privacy protection because social norms adjust to the status quo).

73. *Cf.* Erin Todd Bronchetti et al., *When a Nudge Isn't Enough: Defaults and Saving Among Low-Income Tax Filers* (Nat'l Bureau of Econ. Research, Working Paper No. 16887, 2011), *available at* http://www.nber.org/papers/w16887 (finding that placing part of tax refund in a savings vehicle by default had no effect on whether taxpayer saved the funds, and suggesting that the result was because taxpayers had well-understood preexisting preferences about whether to save or spend the funds).

74. *See, e.g.*, Korobkin, *supra* note 52, at 1622 (presenting evidence that when preference uncertainty is removed, defaults lose their power); Asa Lofgren et al., *Are Experienced People Affected by a Pre-Set Default Option—Results from a Field Experiment*, 63 J. ENVIRON. ECON. &

But when consumers do not understand their options or their preferences, consumers are more susceptible to the mechanisms that make defaults sticky.[75] The personal-data-tracking arena has both of these features, and thus is one in which defaults can be powerful.[76]

Most consumers understand their information privacy options poorly.[77] The variety of data that can be collected through tracking, the host of entities that can collect or obtain that data, the ways that data can be used, and the potential costs and benefits of data collection are bewildering. The intangible effects of tracking are nigh impossible to assess; for example, most people probably cannot forecast whether any particular tracking will make them feel watched or how such a feeling will impact their lives.[78] Even as to concrete effects, people do not know—and cannot know—what effect their data will have on pricing, access to employment, or chances of identity theft.[79] This complexity defies simplification. One set of researchers, who found that simplifying the language and formatting of privacy policies barely improved

MGMT. 66 (2012) (finding that people who know what they want through experience with a decision are less affected by defaults).

75. *See, e.g.*, Sarah Lichtenstein & Paul Slovic, *The Construction of Preference: An Overview*, *in* THE CONSTRUCTION OF PREFERENCE 1 (Sarah Lichtenstein & Paul Slovic eds., 2006) (observing that judgment and decision biases are strongest when preferences are uncertain); Samuelson & Zeckhauser, *supra* note 51, at 29 (finding that choice difficulty increases the pull of defaults); *id.* at 8 (finding subjects more susceptible to biases favoring the status quo when their preferences are weaker). Other academics have described this process a bit differently, claiming that when consumers lack preexisting preferences, they construct preferences in the course of decision making, and that the framing of the decision through the presence of a default shapes how that preference is constructed. But, a position's status as a default does not alone drive consumers towards that position; rather, the mechanisms that can make defaults sticky must come into play. *See* Julie R. Agnew et al., *Who Chooses Annuities? An Experimental Investigation of the Role of Gender, Framing and Defaults*, 98 AM. ECON. REV. 418, 421 (2008) (finding experimentally that defaults have no effect when transaction barriers, biases, and preference formation effects are absent). Further, many of these mechanisms can lead a consumer to remain in a default position without affecting her preferences; a consumer who sticks with a default due to transaction costs or salience effects does not necessarily prefer the default over the opt-out position, *ceterus paribus*.

76. *Cf.* Eric J. Johnson et al., *Defaults, Framing and Privacy: Why Opting In ≠ Opting Out*, 13 MARKETING LETTERS 5 (2002) (finding large default effect in a privacy-related experiment, and suggesting that people's uncertainty about their preferences contributes to the power of privacy defaults).

77. *Cf.* Jensen et al., *supra* note 30 (finding that consumers have little understanding of even well-publicized privacy-related technologies, such as cookies).

78. *See, e.g.*, Ur et al., *supra* note 49; Aleecia M. McDonald & Lorrie Faith Cranor, *An Empirical Study of How People Perceive Online Behavioral Advertising* (Carnegie Mellon Univ., Working Paper CMU-CyLab-09-015, 2009), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09015.pdf.

79. *See, e.g.*, Alessandro Acquisti & Jens Grossklags, *Uncertainty, Ambiguity and Privacy*, COMM. & STRATEGY 6 (2012).

consumer comprehension, explains, "even the most readable policies are too difficult for most people to understand and even the best policies are confusing."[80]

Most consumers have a similarly poor grasp of their own privacy preferences and what actions are necessary to meet those preferences. Even consumers who describe themselves as highly valuing privacy act in ways that reveal abundant private information; in one experiment, many consumers who said they wanted to keep information about themselves private revealed that very information when asked for it by an interactive computer figure on a commercial website.[81] Consumers also have competing preferences. For example, they find tracking for advertising purposes scary and creepy yet also smart and useful.[82] They cannot make the tradeoffs between the incommensurable costs and benefits of privacy; they want to keep their personal information private *and* they want the benefits made possible by revealing that information. One survey's findings are telling: 84% of consumers say they would rather receive targeted advertising in exchange for online content than to pay for online content with money, but 93% of these same consumers say that they would opt into a Don't-Track-Me position if given the choice.[83]

III. DEFAULTS IN THEORY

Observing that people tend to stick with default settings, particularly when they are uncertain about their options and their preferences, academics have claimed that defaults can further policy objectives. This Part explains the theory behind this claim. It then describes how policymakers appear likely to translate this theory into practice in the data privacy policy arena.

A. THE THEORY BEHIND THE USE OF DEFAULTS IN POLICYMAKING

Academics have suggested that defaults can be used in policymaking in two ways: to increase the number of people in the default position (policy

80. Aleecia M. McDonald et al., *A Comparative Study of Online Privacy Policies and Formats*, 5672 LECTURE NOTES IN COMPUTER SCI. 37, 52 (2009).

81. *See* Sarah Spiekermann et al., *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior* § 3.3 (2002), http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf.

82. Ur et al., *supra* note 49, at 6; *see also* Ronald Brownstein, *Americans Know They've Already Lost Their Privacy*, NAT'L J. (June 13, 2013), *available at* http://www.nationaljournal.com/next-economy/big-questions/americans-know-they-ve-already-lost-their-privacy-20130613 (finding widespread consumer ambivalence about the effects of personal information sharing).

83. Annalect Research Group, *supra* note 43, at 2.

defaults) or to provide firms with incentives to educate people about the default (penalty defaults).[84] To ensure that policy defaults are sticky for consumers with weak preferences but not for those who truly prefer the opt-out position, and to ensure that penalty defaults are information-forcing, policymakers have sought to employ a variety of altering and framing rules.

1. Policy Defaults

Policy defaults are put in place with the explicit goal of increasing the number of people in the default position.[85] The idea is to set the default to a position that is good for most individuals,[86] under the assumptions that the majority will keep the default setting and that only the minority who have contrary preferences will reject it. The default in theory will guide uncertain individuals to the position that is best for most people but will not prevent those who know they have contrary preferences from opting out.

The iconic case of a policy default is automatic enrollment in defined contribution retirement savings plans, which is believed to be the best position for the vast majority of employees.[87] Employers that have made participation in their plans the default have increased their employee participation rates by forty percent or more.[88] Another example is the default for checking account overdraft coverage, which, in effect, prohibits banks from providing a consumer with expensive overdraft coverage for ATM and nonrecurring debit card transactions unless the consumer opts out of a no-overdraft default setting.[89] Regulators enacted this default scheme on the theory that the default position is best for most consumers, and the few consumers who benefit from overdraft coverage can opt out.[90]

84. *See, e.g.*, THALER & SUNSTEIN, *supra* note 21 (advocating the use of policy defaults); Ayres & Gertner, *supra* note 15, at 91 (advocating the use of penalty defaults).

85. *Accord* McKenzie et al., *supra* note 14.

86. *See* Janger & Schwartz, *supra* note 15, at 1236, 1245–46 (using "majoritarian defaults" to refer to default positions set to what the policymaker believes the majority of relevant parties would want and "normative defaults" to refer to default positions set to what the policymaker believes is best for society).

87. *See, e.g.*, THALER & SUNSTEIN, *supra* note 21; John Beshears et al., *Public Policy and Saving for Retirement: The "Autosave" Features of the Pension Protection Act of 2006*, *in* BETTER LIVING THROUGH ECONOMICS 274, 287 (John G. Seigfried ed., 2010) (quoting Peter Orszag as "declar[ing] the autosave features of the Pension Protection Act 'a stunning example of the success of behavioral economics in effecting public policy' ").

88. *See, e.g.*, William E. Nessmith et al., *Measuring the Effectiveness of Automatic Enrollment*, 31 VANGUARD CENTER FOR RETIREMENT RES. RPT. 6 (2007).

89. 12 C.F.R. § 205 (2014).

90. *Id.*

2. Penalty Defaults

Penalty defaults correct information asymmetries between parties, such as those that commonly exist between firms and consumers. Policymakers set the default to a position disliked by firms, on the premise that firms that want consumers to opt out will be forced to reveal the default and negotiate with consumers.[91] Like policy defaults, penalty defaults respond to the evidence that less knowledgeable consumers are most frequently affected by the default. Firm efforts to explain the default and opt-out positions so as to convince consumers to opt out will, in theory, educate precisely those consumers who need to know more about the default to make a good decision.

Two well-known penalty defaults are the warranties of merchantability[92] and fitness for a particular purpose[93] under the Uniform Commercial Code. The penalty default is that the warranties will apply; a seller that does not want the warranties to be part of the contract for sale must explicitly opt out.[94] The checking account overdraft coverage default could also be a penalty default. If the bank wants consumers to pay the affected types of overdraft fees, it will be forced to explain how overdraft coverage works in the process of convincing consumers to opt out of the default.

3. Altering and Framing Rules

Policymakers attempt to manage the stickiness, slipperiness, and informativeness of defaults through altering and framing rules. Altering rules tinker with the process for opting out. For example, an altering rule might require that a consumer be able to opt out with a single click, or might require a consumer to complete many steps to opt out. Framing rules attempt to manage the presentation of the default and opt-out option to the user, whether by architecture or messaging. Architecturally, for example, a software default setting could be made more or less salient through the positioning of opt-out controls, hidden deep inside multiple menus or popping up in a nagging window on the screen. Opting out of a default also might be made more or less attractive through messages to the user. For example, an alert or notice box might suggest that the user change a software

91. *See* Ayres & Gertner, *supra* note 15, at 91; *see also* Janger & Schwartz, *supra* note 15, at 1239 (dubbing penalty defaults "information-forcing defaults").

92. U.C.C. § 2-314 (2013).

93. *Id.* § 2-315.

94. *Id.* § 2-316. Note that in the consumer context, the Magnuson Moss Act restricts the degree to which these default warranties can be disclaimed. *See* 15 U.S.C. § 2301 *et seq.* (2012).

setting or instead warn the user that changing the setting could cause problems.

Where a default might otherwise be too sticky, altering rules might aim to keep the costs of opting out low and the process for opting out simple. Framing rules might aim to keep the option to opt out visible. But where policymakers fear that a default will be too slippery and will not be information-forcing, they might set altering rules that impose transaction costs on opting out and framing rules that require the provision of information as a precondition of opting out. Altering and framing rules reflect some awareness that defaults alone will not achieve policymakers' desired ends. Theoretically, carefully calibrated altering and framing rules make policy and penalty defaults work properly.[95]

Two examples show how these rules are employed. In the case of automatic enrollment in retirement savings plans, policymakers are concerned that the default could be too sticky. Altering and framing rules therefore require employers to give employees who are enrolled by default written notices of the right to opt out at specified intervals. These notices must be written at a level that the average employee can understand so that the opportunity to opt out is not confusing or invisible.[96] In contrast, policymakers are concerned that the default for checking account overdraft coverage on ATM and debit transactions could be too slippery and might not be information-forcing.[97] Therefore, framing rules require banks to give accountholders notices explaining the potential costs of opting out of the default and into overdraft coverage—notices that must be segregated from other account documents.[98] Altering rules require banks to provide the same

95. *Cf.* Ayres, *supra* note 16, at 2044–45 (explaining that altering rules can be used to "enhance contractual efficiency and equity" and/or to "manage and restrain negative externalities and internalities while simultaneously permitting opt-out for a subset of contractors who, at least as a group, pass a social cost benefit test").

96. 26 C.F.R. § 1.401(k)–3(d)(3) (2014) ("The content requirement . . . is satisfied if the notice is—(A) Sufficiently accurate and comprehensive . . . (B) Written in a manner calculated to be understood by the average employee . . . .").

97. *See* Electronic Fund Transfers, 12 C.F.R. § 205.17(b) (2014). An overdraft occurs when an accountholder attempts to withdraw more from her checking account than is available, and the bank covers the withdrawal and then reimburses itself when the next deposit is made into the account. For what amounts to a short-term loan the bank charges the accountholder a fee, one that is frequently larger than the amount borrowed. *See* FED. DEPOSIT INSURANCE CORP., FDIC STUDY OF BANK OVERDRAFT PROGRAMS 20 tbl.IV–9 (2008), http://www.fdic.gov/bank/analytical/overdraft/FDIC138_Report_Final_v508.pdf (finding in a 2007 survey of banks that the median negative balance from a debit transaction on which an overdraft fee was charged was about twenty dollars and the median fee was twenty-seven dollars).

98. 12 C.F.R. § 205.17(d) (2014).

account terms, conditions, and features to accountholders who do and do not keep the default setting.[99] They also prohibit banks from opting consumers out in routinely unread fine print; consumers must affirmatively opt out.[100]

4. An Aside on Forced Choice

In addition to Track-Me or Don't-Track-Me defaults, a third possibility is forced choice, meaning consumers could not continue with the online or off-line activity from which data will be collected without affirmatively making choices about tracking.[101] Under a forced choice regime, a consumer could not enter a store that tracks cellphones, view a website that tracks browsing activity, use a credit card at a retailer that tracks customer purchases, or open a mobile device application that collects personal data without first deciding whether to be tracked. Forced choice could be attractive where policymakers believe consumers have diverse well-informed preferences that ought to be honored.

However, forced choice does not work well when people are uncertain about their preferences and options, and would be terribly burdensome for consumers if applied to every situation in which a firm wanted to track a consumer.[102] Forced choice would mean that every consumer decision about tracking would be narrowly-bracketed, which, as explained previously, favors the Track-Me position. In fact, as explained below, firms that benefit from tracking consumers would doubtless respond to a Don't-Track-Me default by repeatedly asking consumers to opt-out, creating a scenario similar to forced choice. Most consumers would respond with a reflexive "yes" click so as to move along in their daily activities rather than engage in reflective decision making.[103]

---

99. *Id.* § 205.17(b)(3).

100. *Id.* § 205.17(b)(1)(iii).

101. *See* Sunstein, *supra* note 11 at 18 ("Another possibility would be to ask customers—the first time they open the browser or periodically—about the privacy setting that that they prefer, and perhaps to prevent them from proceeding until they answer."). "Forced" or "mandated" choice is also called "active choosing." *See id.*

102. *See id.* at 21 ("Suppose that the situation is unfamiliar and complicated. Suppose that people lack information or experience. If so, active choosing may impose unjustified or excessive costs on people; it might produce frustration and appear to require pointless red-tape.").

103. In the abstract, the occasional forced choice might be somewhat successful in improving the quality of consumer choice. But this presents a coordination problem, given that no firm will know whether another firm has recently asked a consumer to make a decision about tracking.

B. TRANSLATING DEFAULT THEORY TO TRACKING POLICY

Translating the theory behind the use of defaults in policymaking into practice in the personal-data-tracking context quickly reveals that the academic literature is incomplete. That literature addresses what the position of the default setting ought to be and, roughly, how altering and framing rules ought to be set, but does not address a necessary prior question—the scope of the default setting. It also does not address the granularity of opt-out choices consumers ought to be given.

The following describes the tracking default positions that the theory behind the use of defaults in policymaking might support. It also explores the scope of these default positions, the opt-out choices, and the accompanying altering and framing rules that policymakers appear poised to enact. To do this, it draws primarily from two sources. First, the preliminary draft of the default scheme for tracking of information about individuals' use of the Internet and mobile devices[104] developed by the World Wide Web Consortium ("W3C"), an international body that sets voluntary, widely-adopted technological standards intended "to lead the World Wide Web to its full potential."[105] Second, the proposals made by the Federal Trade Commission ("FTC") for the collection or use of consumer data that can reasonably be linked to particular consumers, computers, or devices.[106] The

104. The current draft scheme is described in two documents: WORLD WIDE WEB CONSORTIUM, TRACKING COMPLIANCE AND SCOPE: W3C WORKING DRAFT, http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html (last visited Aug. 15, 2013) [hereinafter W3C TCS], and WORLD WIDE WEB CONSORTIUM, TRACKING PREFERENCE EXPRESSION (DNT)—W3C WORKING DRAFT, http://www.w3.org/TR/tracking-dnt (last visited Aug. 15, 2013) [hereinafter W3C TPE].

105. W3C Mission, http://www.w3.org/Consortium/mission (last visited Nov. 25, 2013); *see also* ABOUT W3C, http://www.w3.org/Consortium (last visited Nov. 25, 2013) ("The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards."). The W3C is not a body of elected policymakers, but rather a consortium of industry, consumer, and government representatives that seek to develop standards by consensus. The body has no regulatory authority, and must depend on the makers of devices, servers, browsers, and applications to voluntarily implement its standards. However, if it were to come to an agreement on tracking standards, policymakers might well adopt these standards into the law. *But see* Blair Reeves, *Online Advertising, BATNAs & the Failure of Do Not Track*, CLICKZ (Oct. 28, 2013), *available at* http://www.clickz.com/clickz/column/2302960/online-advertising-batnas-the-failure-of-do-not-track (expressing skepticism that the W3C will come to consensus on a tracking standard).

106. These two proposals are contained in: FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE vii, 35–59 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC PRIVACY REPORT]; FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES 21 (2013), *available at*

W3C and FTC proposals are not legally binding, but default-minded legislators will certainly look to these sources when formulating privacy policy.

1. Scope of Tracking Defaults

The theory behind policy and penalty defaults assumes that defaults are transparently binary—one is either in a clear default position or one is not. But the tracking arena presents a particularly acute example of how complex and unintuitive a default and/or opt-out position might be. This is because "tracking" encompasses a very wide variety of personal data collection practices, and these practices have different costs and benefits depending on, for example:

- types of information collected (e.g., geolocation data, clickstream data,[107] medical data, email content),
- uses of information (e.g., medical research, marketing, pricing, website use analytics, employment),
- collection sites (e.g., particular websites, mobile applications),
- types of users of information (e.g., first-parties, meaning the firms with which consumers know they are interacting, such as wireless service providers and the firms that run websites; affiliates of first-parties; or third-parties to which first-parties sell data or access to data[108]), and
- individual users (particular firms or other entities).[109]

Policymakers could set the default broadly to Track-Me (or Don't-Track-Me) for most of these dimensions. Alternatively, they could set a mix of narrower defaults and unalterable positions.

---

http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf [hereinafter FTC MOBILE REPORT].

107. Clickstream data refers to the information generated by users' mouse movements and clicks through the website they visit, as well as the sites visited, duration of the visit, and order of site visits. *Definition: Clickstream Analysis*, SEARCHCRM, http://searchcrm.techtarget.com/definition/clickstream-analysis (last visited Aug. 1, 2013).

108. But given that third parties can become affiliates of first parties and that first parties can act as the handmaidens of third parties, tracking defaults that turn on these distinctions may be subverted. *Cf.* Mitch Weinstein, *Why Blocking Third-Party Cookies Is Good for Google and Facebook*, ADEXCHANGER (June 20, 2013), http://www.adexchanger.com/data-driven-thinking/why-blocking-third-party-cookies-is-good-for-google-and-facebook.

109. Policymakers could regulate the original collection of data, downstream users, or uses. Enforcement concerns would push toward limiting the original collection of data, even where only some potential downstream users or uses are problematic. However, to present the strongest case for the use of tracking defaults, this Article sets aside these enforcement concerns. *See supra* note 10 and accompanying text.

Consider the decision about whether to require firms to give consumers choice, or to set (or allow firms to set) an unalterable position. For some information, policymakers might decide that the costs of tracking outweigh the benefits, regardless of consumer preferences, and therefore set an unalterable Don't-Track-Me position. For example, policymakers might generally prohibit the tracking of sexual orientation or medical data for employment purposes. For other data, policymakers might decide that the benefits of tracking outweigh the costs, and therefore set an unalterable Track-Me position. For example, firms might be permitted to track clickstream data for website analytics purposes, without giving consumers an ability to opt out.

The broader the default scope, the more easily it can be understood, but the more likely that it will not satisfy most consumer preferences. For example, a Don't-Track-Me default that prohibits all passive personal data collection is intuitive, but most consumers want some tracking for some purposes (e.g., order fulfillment, fraud prevention, or clickstream data tracking for the purposes of pre- or re-populating online forms). A broad setting could thus lead most consumers to try to opt out to some extent, defeating the premise of policy defaults that inertia should lead most consumers to the best position. A broad default that leads most consumers to try to partially opt out could also founder if consumers are confused about their opt-out choices. For example, consumers might have the impression they must accept all tracking to receive the benefit of pre-populated online forms.

Existing tracking proposals therefore attempt to discern which position substantial majorities of consumers would want to be in with respect to each type of information, type of user, etc., and make these unalterable; but where consumers are more heterogeneous in their preferences, the proposals give consumers a choice. The current W3C draft proposal allows consumers to opt out of third-party tracking of geolocation data more granular than the zip-code level and of third-party tracking of other data when used for certain purposes, such as behavioral advertising. First parties could continue to collect any consumer data and could customize content and advertising based on the consumer's interaction with that firm.[110] Under the W3C draft proposal, consumers cannot opt out of any tracking by first parties, tracking of gross geolocation data by any party, or tracking for "permissible

110. W3C TCS, *supra* note 104, § 4.

purposes" by third parties.[111] Similarly, the FTC tracking proposal allows first parties to collect and use information about consumers without giving consumers an opportunity to opt out where "the practice [of data collection and use] is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law."[112] Contextually-appropriate uses not requiring consumer choice include the collection and use of data for the purposes of "fulfillment, fraud prevention, internal operations, . . . and most first-party marketing."[113]

While the precise contours of the scope of the defaults policymakers would adopt are unclear, what is clear is that there are some categories of information tracking from which consumers will not be permitted to opt out. As discussed further below, allowing consumers to opt out of some but not all tracking is likely to confuse consumers and lead some to feel that opting out is futile.

2. Setting: Track-Me or Don't-Track-Me

Within the set of potentially-tracked information about which policymakers wish to give consumers control, policymakers then must decide which defaults should be Track-Me and which should be Don't-Track-Me. If policymakers believe tracking produces more privacy benefits than harms (for example, in the form of financial support for Internet content or application development), they might support a Track-Me default. Because in this scenario policymakers believe that the majority ought to be in the Track-Me position,[114] it would be a policy default.

On the other hand, if policymakers believe that tracking produces more potential privacy harms than benefits (for example, in the form of increased risk of identity theft or decreased space for individual experimentation and growth), they might support a Don't-Track-Me default. Because they believe that the untracked position is best for most people, these policymakers would look for a policy-default effect, meaning that the majority would stick with this default position but those with strong contrary preferences would

111. "Permissible purposes" include frequency capping (measuring how many times a consumer has been shown an ad), billing (to ensure third-party advertisers are paying first-party websites correctly), and debugging. *Id.* § 5.

112. FTC PRIVACY REPORT, *supra* note 106, at 38–39.

113. *Id.* at 39.

114. Policymakers might support a Track-Me default on political expediency or other grounds as well, but this discussion focuses on the tracking default setting that the theory underlying the use of defaults in policymaking would support.

opt out. Many supporters of Don't-Track-Me defaults appear to aim for a policy-default effect.[115]

Policymakers who are uncertain about the social welfare effects of tracking or believe that people have heterogeneous preferences about tracking, also might support a Don't-Track-Me default. Personal-information tracking presents a case of information asymmetry, where one party (the firm) is well informed and the other (the consumer) is poorly informed. Because the business model of many Internet and mobile-application firms depends on the revenue firms can obtain through the sale of tracked information, firms have a strong interest in placing consumers in a Track-Me position.[116] Thus, a policymaker might intend for the Don't-Track-Me default to operate as a penalty default so that firms reveal this default position to consumers in the process of urging consumers to opt out. Consumers would then be free to make informed decisions about whether they want to be tracked. Academics in particular have argued for various forms of Don't-Track-Me defaults on this basis.[117]

Defaults could be set narrowly, with a different setting for each potential combination of data attributes listed above (i.e., type of information, information use, collection site, etc.). For example, the default for collection of health information by third parties for purposes other than diagnosis, treatment, or research could be Don't-Track-Me, but the default for

115. *See, e.g.*, Chris Soghoian, *End the Charade: Regulators Must Protect Users' Privacy by Default*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2010), http://www.priv.gc.ca/information/research-recherche/2010/soghoian_201012_e.asp (implying that a Don't-Track-Me default would be so sticky that advertisers would be forced to abandon behavioral advertising); Tene & Polonetsky, *supra* note 20 (suggesting that supporters of Don't-Track-Me defaults aim to keep people in the Don't-Track-Me position rather than to give people a choice).

116. *See, e.g.*, Vindu Goel, *Facebook Eases Privacy Rules for Teenagers*, N.Y. TIMES, Oct. 16, 2013, http://www.nytimes.com/2013/10/17/technology/facebook-changes-privacy-policy-for-teenagers.html ("But fundamentally, Facebook wants to encourage more public sharing, not less. The company, which has about its 1.2 billion users worldwide, is locked in a battle with Twitter and Google to attract consumer advertisers like food, phone and clothing companies."); James Temple, *Rules Against Tracking Don't Go Far Enough*, SAN FRANCISCO CHRON., Mar. 7, 2012, http://www.sfgate.com/business/article/Rules-against-online-tracking-don-t-go-far-enough-3387373.php ("Targeting ads based on search queries, sites visited, stories read and social connections forms the core of the multimillion-dollar business models of many online companies, including Google, Yahoo and Facebook.").

117. *See, e.g.*, Kesan & Shah, *supra* note 12, at 621 (arguing that setting browser defaults to reject cookies "would ensure that people understood the privacy risks of cookies"); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2100 (2004) ("This Article prefers an opt-in default because . . . it would place pressure on the better-informed party to disclose material information about how personal data will be used. This default promises to force the disclosure of hidden information about data-processing practices.").

collection by first parties or for diagnosis, treatment, or research purposes could be Track-Me. Such narrow defaults might respond to reasonable cost-benefit assessments of different tracking practices, but narrow defaults increase the likelihood that consumers will be confused about how the default works.

Existing proposals therefore suggest broader settings. The W3C preliminary draft proposal contemplates that Track-Me would be the default for all tracking, a policy default.[118] The FTC suggests a Don't-Track-Me default for all collection of sensitive information—"information about children, financial and health information, Social Security numbers, and precise geolocation data"—requiring express consent from consumers before the information can be collected.[119] For all other tracking over which consumers are given control—i.e., the collection of non-sensitive information by third parties (or affiliates of first parties where the affiliate relationship is not obvious to consumers) or by first parties tracking consumers across third-party websites, or for first parties sharing non-sensitive information with third parties—the FTC's proposed default is Track-Me.[120]

While the particular settings of the defaults policymakers would adopt is again unknown, it seems probable that policymakers will adopt a mix of Track-Me and Don't-Track-Me positions for those data collection practices that are within the control of the consumer. As discussed further below, this mix of settings could be confusing for many consumers. Its precision could also create the appearance that policymakers have carefully determined which collection practices are potentially harmful and which present no danger of harm, and have assigned each to a Don't-Track-Me or Track-Me default accordingly, potentially lulling consumers into a false sense that the default settings will protect them from any harm from tracking.

3. Granularity of Available Opt-Out Positions

Once policymakers decide to allow consumers to opt out of a particular type of information tracking, they then must decide the scope of the opt-out mechanism. Opting out of a default wholesale might be the only alternative given to consumers, or consumers might be permitted to opt out narrowly.

118. The W3C draft default requires general purpose browsers to be initially set to "Track-Me" or "No Preference," either of which would permit tracking. W3C TPE, *supra* note 104, § 3. However, a consumer can opt out by using a special-purpose browser that is marketed as a privacy-enhancing technology. *Id.*

119. FTC PRIVACY REPORT, *supra* note 106, at 59.

120. *Id.* at 40–42.

For example, a consumer might be given the power to decline tracking by third parties while accepting tracking by first parties, or to choose whether to be tracked on a website-by-website basis. To the extent that tracking is performed through cookie technology, common web browser setting choices today give consumers the ability to opt out on both of these bases. For example, in Firefox a consumer can choose to accept all cookies, accept no cookies, accept cookies from first parties but not from third parties, or make exceptions from each of these for particular websites.[121]

The broader the opt-out mechanism, the more easily it is understood by consumers, but the more likely that consumers will be unable to satisfy their textured preferences. Switching positions wholesale from Track-Me to Don't-Track-Me or vice versa each time a consumer encounters a tracking practice for which she wants a different setting is onerous and can lead to mistakes. For example, if a consumer in a Don't-Track-Me position changes tracking settings wholesale to facilitate a particular transaction, she must go back and change settings again to return to a Don't-Track-Me position, a step she may not remember to perform. A granular set of selective opt-out options would allow sophisticated consumers to satisfy particular preferences but presents the danger of overwhelming the average consumer.[122]

Given that the overarching goal of the use of personal data defaults is to facilitate individual choice about whether, when, and by whom to be tracked, policymakers will no doubt create a scheme by which consumers can selectively opt in or out of tracking defaults. The W3C and FTC proposals all permit consumers to, in effect, opt out on a firm-by-firm basis. For example, the FTC mobile device proposal suggests that the default for most information be Track-Me, that consumers be permitted to opt out from this wholesale, but that consumers then be permitted to opt back into tracking on an application-by-application basis:

> A DNT setting placed at the platform level could give consumers . . . a way to control the transmission of information to third parties as consumers are using apps on their mobile devices . . . . Offering this setting or control through the platform will allow consumers to make a one-time selection rather than having to

121. *See Block Websites from Storing Site Preferences or Login Status in Firefox*, MOZILLA SUPPORT, https://support.mozilla.org/en-US/kb/block-websites-storing-site-preferences (last visited Nov. 25, 2013). As previously noted, however, trackers can track through other means than cookies, such as through digital fingerprinting. *See* Tanner, *supra* note 33.

122. For example, when Facebook added more granular privacy controls, users became confused and more users kept the default settings. *See* Fred Stutzman et al., *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY 2, 23 (2013).

> make decisions on an app-by-app basis. Apps that wish to offer services to consumers that are supported by behavioral advertising would remain free to engage potential customers in a dialogue to explain the value of behavioral tracking and obtain consent to engage in such tracking.[123]

The W3C draft proposal is similar.[124] If the default were Don't-Track-Me, a comparable scheme might give consumers both a wholesale opt-out choice, allowing them to opt into the Track-Me position with respect to all firms, and granular choices, allowing them to agree to tracking on a firm-by-firm basis.

4. Altering and Framing Rules

Policymakers would then need to select altering and framing rules for these defaults. Recall that the goals of such rules are to prevent the default from being too sticky or too slippery and to inform consumers about the default and option to opt out. Given that the tracking defaults and opt-out choices policymakers appear inclined to embrace are complex, ensuring that consumers understand their choices and are able to act on them is a demanding task. While the theoretically possible altering and framing rules are limitless, this section sketches the general contours of rules that are on the horizon.

First, policymakers will put framing rules in place that aim to make the default and opportunity to opt out salient. For example, framing rules might require the default and opportunity to opt out to be "prominent"[125]—disclosed in words that "are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear."[126] The FTC proposal suggests that the choice to opt out should be given to consumers "at a time and in a context relevant to the consumer's decision about whether to allow data collection and use," such as "directly adjacent to where the consumer is entering his or her data" online, "immediately upon signing up for a service," or, for an offline transaction, "close to the time of sale"

123. FTC MOBILE REPORT, *supra* note 106, at 21.

124. W3C TPE, *supra* note 104, § 6.

125. *See* FTC PRIVACY REPORT, *supra* note 106, at 50; *see also* Decision and Order, *In re* ScanScout, Inc., File No. 1023185 (Fed. Trade Comm'n Dec. 14, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutdo.pdf [hereinafter ScanScout Consent Order] (requiring "prominent" placement of a notification about a default and opt-out mechanism).

126. ScanScout Consent Order, *supra* note 125.

through notification on a "sales receipt" or "prominent poster at the location where the transaction takes place."[127]

Second, to forestall confusion, policymakers will enact altering rules that require the mechanism for opting out to be "easy to find and use."[128] More particularly, firms might be required to create an opt-out process that involves no more than one or two clicks of a button to opt out.[129] The opt-out process might be standardized, at least to some extent, across browsers, websites, mobile devices, or applications. Or, the process for opting back into the default after having opted out might be regulated so that firms cannot change a consumer's position through unread fine print. For example, while the W3C draft default scheme does not contain rules regarding the process for opting out of the default,[130] it would require that where a consumer has opted out at the browser level, opting back in to a Track-Me position with respect to any particular firm should be done "explicit[ly]."[131]

These rules aimed at salience and eliminating confusion would work simultaneously to inform consumers about the default and the opt-out opportunity. For example, the W3C preliminary draft requires firms that track consumers and all browsers to "clearly and accurately" with a "brief and neutral explanatory text" explain three things: (1) a consumer can opt out of some third-party tracking, (2) a consumer who has opted out may continue to be tracked for "permissible" purposes, and (3) a consumer who has opted out at the browser level can opt back in with respect to a particular

127. FTC PRIVACY REPORT, *supra* note 106, at 50.

128. FTC MOBILE REPORT, *supra* note 106, at 21.

129. *See* ScanScout Consent Order, *supra* note 125.

130. *See* W3C TPE, *supra* note 104, § 3. The draft states:

> We do not specify how tracking preference choices are offered to the user or how the preference is enabled: each implementation is responsible for determining the user experience by which a tracking preference is enabled. For example, a user might select a check-box in their user agent's configuration, install an extension or add-on that is specifically designed to add a tracking preference expression, or make a choice for privacy that then implicitly includes a tracking preference (e.g., Privacy settings: high). The user-agent might ask the user for their preference during startup, perhaps on first use or after an update adds the tracking protection feature. Likewise, a user might install or configure a proxy to add the expression to their own outgoing requests.

Id.

131. W3C TCS, *supra* note 104, § 6.

firm.[132] Where a consumer has opted out of tracking at the browser level, the consumer's opting back in selectively would need to be "informed."[133]

Third, policymakers might put altering rules in place intended to minimize the costs of opting out. For example, rules might require that consumers be given a "universal" opt-out mechanism at the browser level or, if technologically feasible, the device level.[134] (A universal mechanism would also present consumers with a broadly-bracketed choice, perhaps leading to more privacy-minded decisions.) To keep the cost of opting out low, rules might require the opt-out mechanism be "persistent,"[135] meaning that firms could not require consumers to opt out repeatedly the way that cookie-based opt-out systems do today.

In theory, a default scheme might also prohibit firms from giving consumers incentives to agree to tracking. The law might require firms to treat consumers in the Don't-Track-Me position the same as consumers in the Track-Me position, regardless of the particular purposes for which the firm tracks consumers. However, when the content and features of a website or app depend on revenue generated by tracking, as many currently do, policymakers will be reluctant to undermine this arrangement. For this reason, the W3C preliminary draft explicitly permits firms to condition services on consumers agreeing to be tracked.[136] With a narrow exception for "important product[s] with few substitutes, such as a patented medical device," the FTC proposal also asserts that firms should be permitted to condition access to goods, services, website content, etc. on consumers agreeing to tracking and to offer tracked consumers lower prices or other benefits.[137]

Moreover, policing the line between differential treatment intended to force consumers to agree to tracking and differential treatment that is the necessary consequence of refusing to be tracked would be difficult. Apps or websites could be optimized to function when tracking is enabled, as some websites already do today. For example, many websites warn consumers: "If you turn cookies off, you will not have access to many features that make

132. *Id.* § 3.

133. *Id.* § 6.

134. FTC MOBILE REPORT, *supra* note 106, at 21 (suggesting a universal mechanism to opt out of the Track-Me default be made available at the mobile device level).

135. *Id.*

136. W3C TPE, *supra* note 104, § 1 ("Web sites that are unwilling or unable to offer content without such targeted advertising or data collection need a mechanism to indicate those requirements to the user and allow them (or their user agent) to make an individual choice regarding exceptions.").

137. FTC PRIVACY REPORT, *supra* note 106, at 52.

your user experience more efficient and some parts of our website will not function properly."[138] One goes so far as to warn consumers that choosing not to be tracked will "spoil[] your experience of the website."[139] Google's "Privacy Policy" specifically indicates that its search engine might not display websites in the consumer's language automatically if the consumer disables cookies.[140] Alternatively, a website might deliver behaviorally-targeted ads to consenting consumers and a larger quantity of particularly distracting generic ads to untracked consumers. It might not be possible to detect when the larger quantity or greater distraction is necessary to produce revenue equivalent to behavioral ads and when it is harassment to induce consumers to agree to tracking. Thus, even if altering rules prohibited treating consumers who refuse to be tracked any differently than consumers who agree to be tracked, enforcing this prohibition would likely prove impossible.

* * *

In sum, while the precise default scope, settings, opt-out options, and altering and framing rules policymakers would choose if they were to enact a tracking default scheme are not certain, a few key features can be anticipated. These include the following:

1. the scope of the defaults will be limited, in that there will be some tracking from which consumers cannot opt out;
2. the settings will be a mix of Track-Me and Don't-Track-Me defaults;
3. the control consumers are given will be granular; and
4. altering rules will not prohibit trackers from giving consumers incentives to agree to stay in or move to the Track-Me position.

IV. DEFAULTS IN PRACTICE

Defaults in practice do not always live up to the theory behind using defaults in policymaking. This Part describes two failed default schemes,

138. *Consumer Online Privacy Frequently Asked Questions*, U.S. BANK, https://www.usbank.com/privacy/faq.html (last visited July 30, 2013); *see also Disney Registration Cookies Policy*, DISNEY https://registration.disneyinternational.com/cookiepolicy.htm?p=130&fullScreen=true (last visited Nov. 25, 2013) (containing similar warning language); INFORMATION ABOUT COOKIES ON MONSTER, http://inside.monster.com/cookie-info/inside2.aspx (last visited Nov. 25, 2013) (containing a similar warning).

139. *BBC Worldwide—Cookies Policy*, BBCWORLDWIDE.COM, *available at* http://www.bbcworldwide.com/cookies.aspx (last visited Nov. 29, 2013).

140. *Privacy Policy*, GOOGLE, http://www.google.com/policies/privacy (last modified June 24, 2013) ("However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.").

demonstrates how firms have frustrated these schemes by making the defaults too sticky or too slippery, and, through comparison to examples of relatively successful defaults, extracts a set of conditions under which defaults do not perform in accordance with theory.

A. TWO FAILED DEFAULT SCHEMES

Two default schemes that have failed to meet policymaker aims are those for (1) financial institutions' sharing and use of consumer information[141] and (2) banks' charging of overdraft fees for ATM and nonrecurring debit transactions. The former is too sticky and the latter is too slippery. Neither appear to lead to well-informed consumer decisions about whether to stick with the defaults or opt out.[142]

1. The Financial Information Default Scheme

By default, financial institutions collect, use, and share information about their customers for marketing, pricing, and other purposes.[143] Under federal law, consumers can opt out of this in three respects. First, they can opt out to prevent an institution from sharing their personal information with parties that are not affiliated with the institution.[144] Second, they can opt out to prevent an institution from sharing with its affiliates information about the consumer other than information about the institution's own transactions

141. This is not single mandated default but rather collectively represents the requirements of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6802 (prohibiting certain sharing of information with nonaffiliated third parties unless consumers are given the right to opt out), and the requirements of the Fair Credit Reporting Act (FCRA) to avoid being treated as, and therefore subject to the extensive duties placed on, a credit reporting agency, 15 U.S.C. §§ 1681a(d), 1681a(f), 1681s-3 (defining an entity that regularly furnishes consumer reports to others as a consumer reporting agency, but excluding from the definition of consumer report the sharing of certain consumer information among affiliated entities if the consumer is given the option to opt out of this sharing and of the use of this and other information by the affiliate for marketing purposes). The GLBA requires institutions to inform consumers of their GLBA and FCRA opt-out rights. 15 U.S.C. §§ 6803, 6804. For ease of reference, these are treated here as a single default scheme.

142. By other metrics, these defaults may have done some good. For example, they may have led more financial institutions to share less consumer information or more banks to stop charging overdraft fees than would otherwise have occurred. *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 101 (2002) (making this argument as to the financial information defaults). But, by the metrics of well-informed consumer decisions and, for the overdraft default, a significant reduction in overdraft fees for low-income consumers, the ostensible goals of policymakers, these defaults have failed.

143. *See, e.g.*, Fred H. Cate, *Personal Information in Financial Services: The Value of a Balanced Flow*, Financial Services Coordinating Council 3–22 (2000), *available at* http://www.aba.com/aba/PDF/cate.pdf (surveying the many ways in which financial institutions use consumer information).

144. Privacy of Consumer Financial Information, 16 C.F.R. § 313 (2014).

with the consumer.[145] Third, they can opt out to prevent an institution's affiliates from using transaction and "other" information for marketing purposes.[146] Even if a consumer has opted out to the fullest extent, financial institutions can share all gathered information with joint marketing partners, transaction information with affiliates for non-marketing purposes, and "as [further] permitted by law."[147]

The default scheme includes altering and framing rules intended to educate consumers and facilitate opting out. Institutions must allow consumers to opt out at any time and must provide consumers with a "reasonable means" to do so.[148] Institutions must give consumers initial and annual notices explaining their opt-out rights.[149] These notices must be "clear and conspicuous," meaning "reasonably understandable" (in plain language and easy to read) and "designed to call attention to the nature and significance of the information."[150]

But, despite these rules, the financial information defaults are overly sticky and the scheme is not information-forcing. Although consumers generally do not like banks sharing their information with affiliates or third parties,[151] almost no one opts out.[152] Consumers reviewing model explanatory notices in laboratory conditions poorly understand the defaults and opt-out provisions.[153] Comprehension may be even lower under real-world conditions, in which many consumers will not read the notices.

2. The Checking Account Overdraft Default Scheme

As explained above, federal banking regulators effectively require banks to default consumers out of expensive overdraft coverage for ATM and

145. *Id.*
146. *Id.*
147. 16 C.F.R. § 313.15(4) (2014).
148. *Id.* § 313.7.
149. *Id.* § 313.4–.5.
150. *Id.* § 313.3.
151. Cate, *supra* note 143, at 15 (in consumer testing, finding that respondents "do not seem to like their information being shared with nonaffiliates . . . or affiliates").
152. John Martin, *Opting Out—or Not*, ABCNEWS (June 21, 2001), http://more.abcnews.go.com/sections/wnt/dailynews/privacy_notices_010621.html (finding only .5% of people opt out).
153. Alan Levy & Manoj Hastak, *Consumer Comprehension of Financial Privacy Notices*, INTERAGENCY NOTICE PROJECT, 9 tbl.1 (2008), http://ftc.gov/privacy/privacyinitiatives/Levy-Hastak-Report.pdf (showing that less than half the subjects tested were able to select a bank for a cogent and relevant reason based on even the best form notice regulators could develop).

nonrecurring debit card transactions.[154] Altering and framing rules aim to prevent bank "circumvention or evasion" of the default.[155] First, to prevent banks from placing language opting out of the default in routinely unread account disclosures, opting out requires an "affirmative" accountholder action, such as speaking to a bank representative in person or by phone or clicking a box on an online banking form.[156] Second, banks must provide the same account terms, conditions, and features to accountholders who stick with the default as they provide to accountholders who opt out.[157] Framing rules require banks to provide consumers with specific information about the default and the consequences of opting out in a document or webpage segregated from all other documents or webpages.[158]

In promulgating the overdraft default, regulators explicitly stated that they intended for it to operate as a policy default, akin to the auto-enrollment default for retirement savings.[159] But it appears that the majority of the consumers whom regulators intended to assist—low-income frequent users of overdraft[160]—opt out of the default.[161] The rule also does not function as a penalty default; surveys indicate that consumers who opt out hold key misconceptions about the way the default and opt-out positions work.[162]

---

154. Electronic Fund Transfers, 12 C.F.R. § 205.17(b) (2014). Fees on bank-covered overdrafts occasioned by other types of transactions (chiefly checks and recurring payments) are not included in the policy default because these tend to be for necessities and, if not paid, can result in bounced check or late payment fees. *See* Supplement I to Part 205, Official Staff Interpretations of 12 C.F.R. § 205.17(b)(2), cmt. 2 (2014). ATM and nonrecurring debit transactions tend to be discretionary transactions and when these are declined consumers are not charged a fee. Willis, *supra* note 34, at 1180.

155. *See, e.g.*, Electronic Fund Transfers, 74 Fed. Reg. 59,033, 590,44 (Bd. of Governors of the Fed. Reserve Sys. Nov. 17, 2009).

156. *See* One-Time Debit Card Transactions, 12 C.F.R. § 205.17(b)(1)(iii) (2014); 12 C.F.R. pt. 205, supp. I, § 205.17(b)(1)–(4).

157. 12 C.F.R. § 205.17(b)(3).

158. *Id.*

159. Regulators noted that "studies have suggested [that] consumers are likely to adhere to the established default rule, that is, the outcome that would apply if the consumer takes no action" and cited studies of the effectiveness of automatic enrollment in increasing participation in retirement savings plans. Electronic Fund Transfers, 74 Fed. Reg. at 59,038 & n.25.

160. In 2009, one widely-cited industry consultant estimated that ninety percent of overdraft fees were paid by the poorest ten percent of checking accountholders. *See Debit Card Trap*, N.Y. TIMES, Aug. 20, 2009, http://www.nytimes.com/2009/08/20/opinion/20thu1.html (citing Michael Moebs).

161. *See* Willis, *supra* note 34, at 1184.

162. *See* CTR. FOR RESPONSIBLE LENDING, BANKS COLLECT OVERDRAFT OPT-INS THROUGH MISLEADING MARKETING, RESEARCH BRIEF 2, 6 n.8 (2011), *available at* http://www.responsiblelending.org/overdraft-loans/policy-legislation/regulators/CRL-OD-Survey-Brief-final-2-4-25-11.pdf. The brief states:

B. HOW FIRMS MAKE THESE DEFAULTS FAIL

An examination of how financial institutions and banks present these defaults to consumers in practice demonstrates why these defaults have failed to achieve policymaker goals. Institutions work to bolster the mechanisms that can make defaults sticky to ensure that very few consumers opt out of the financial information defaults; banks work to undermine these mechanisms to encourage accountholders to opt out of the overdraft-coverage default.

1. Transaction Barriers

Transaction barriers that can contribute to the stickiness of defaults—costs, confusion, and futility—can be built higher, eliminated, or even inverted.

In the case of the financial information defaults, institutions prefer for consumers to stay in the default information-sharing position, and therefore build high transaction barriers to opting out. For consumers who attempt to opt out, the altering rule requiring "reasonable means" for opting out keeps the transaction costs of doing so for any one institution fairly low.[163] But consumers must opt out with each financial institution with which they have any business. If transaction costs are not enough, institutions warn consumers that opting out will be costly in other ways:

> If you opt out:
>
> We may need you to repeat information that you have already provided and we may not be able to pre-fill applications for you.
>
> We may have to transfer your phone calls more often.

> Sixty percent (60%) of consumers who opted [out of the default] stated that an important reason they did so was to avoid a fee if their debit card was declined. In fact, a declined debit card costs consumers nothing . . . Sixty-four percent (64%) of consumers who opted [out of the default] stated that an important reason they did so was to avoid bouncing paper checks. The truth is that the opt-in rules cover only debit card and ATM transactions.

Id.

163. The only challenge may be that institutions often require consumers to provide account numbers. *See, e.g.*, *Statutory Form of Opt-Out Notice*, FIRST FOUNDATION, https://www.ff-inc.com/privacy/opt-out-notice.aspx (last visited Nov. 25, 2013); *Opting Out of Information Sharing*, METLIFE, https://eforms.metlife.com/wcm8/PDFFiles/730.pdf (last visited Nov. 25, 2013). Locating these might take some time, particularly for closed accounts.

> We may not offer you the products that best meet your needs.[164]

Another transaction barrier is confusion. As noted above, consumers understand the defaults and their opt-out rights poorly, even after reading the required notices. Consumers may not understand that they can opt out at all; even in the flurry of publicity when the notices first went out, fewer than thirty-five percent of consumers surveyed recalled receiving them.[165] Although the law requires that institutions give consumers initial and annual "conspicuous" notices, these arrive with other documents from the institution, documents that may disappear among the reams of disclosures consumers receive, and routinely ignore, in their daily lives.[166]

Finally, financial institutions may capitalize on futility. Even if a consumer has opted out to the fullest extent, financial institutions can continue to share information with joint marketing or other service providers,[167] share information with affiliates for non-marketing purposes,[168] and otherwise share information "as authorized by law."[169] Unable to opt out entirely, consumers might resign themselves to the defaults.

In comparison, banks structure the presentation of the overdraft default and the process for opting out to have the opposite effect. Banks eliminate transaction costs for many consumers and even make it more costly to stick with the default than to opt out. For new customers and for accountholders using online banking, transaction costs do not fortify the default because these costs are the same whether the consumer sticks with the default or opts out; new accountholders in the process of opening an account or existing accountholders attempting to access online banking must check precisely the same number of boxes regardless of whether they check the box for sticking with the default or for opting out.[170] When the default first became law, some banks flooded existing accountholders, particularly those who had

164. *How We Protect You*, UNITED SERVS. AUTO. ASS'N, https://www.usaa.com/inet/ent_references/CpStaticPages?page=ya_efsk_privacyinfo_adult_pub (last visited Apr. 13, 2014).

165. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 360 (Jane Winn ed., 2006) (citing Star Systems, *Financial Privacy: Beyond Title V of Gramm-Leach-Bliley* 9 (2002)).

166. *See* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 665 (2011).

167. 16 C.F.R. § 313.13 (2014).

168. 16 C.F.R. § 313.11.

169. 16 C.F.R. § 313.15(a)(7)(iii).

170. *See* Ben Popken, *Banks Luring You Into Signing Back up for High Overdraft Fees*, THE CONSUMERIST (June 18, 2010), http://con.st/10007945; Phil Villarreal, *When it Comes to Overdraft Opt-In, Chase Won't Take No for an Answer*, THE CONSUMERIST (Aug. 6, 2010), http://con.st/10009792.

overdrafted frequently in the past, with print marketing, in-person bank teller appeals, and telemarketing encouraging them to opt out.[171] The barrage would end only when the consumer opted out,[172] making it costlier to stick with the default—and continue to endure the marketing—than to opt out.[173]

Banks have forestalled the confusion that might otherwise make the overdraft default sticky by ensuring that the opt-out process is salient and easy to use. The volume of overdraft marketing means the option to opt out is difficult to miss. Existing accountholders have been able to opt out by simply pushing a button on an ATM,[174] clicking a button online, or saying "yes" to a bank employee who called to suggest to accountholders that they ought to opt out.[175] Any confusion would run toward opting out, for two reasons. First, banks have framed the opt-out position as a voluntary perk, asking accountholders whether they would like to take advantage of the bank's "courtesy pay"[176] or "account protector"[177] service. Second, banks have capitalized on the fact that the default setting is itself confusing, in that it covers nonrecurring debit and ATM transactions but not checks or recurring debits. Some banks even call overdraft coverage "bounce protection";[178] given that "bounce" is a term usually applied to a dishonored check, the nomenclature probably leads consumers to mistakenly believe that they must opt out in order to receive overdraft coverage for bounced checks.[179]

171. *See* Karen Weise, *Reforms Fail to Halt Bank Revenue on Debit-Card Overdraft Fees*, BLOOMBERG (Oct. 20, 2011), http://www.bloomberg.com/news/2011-10-20/reforms-fail-to-halt-bank-revenue-on-debit-card-overdaft-fees.html; Ben Popken, *Chase Just Goes Ahead and Adds Overdraft Protection to Your Account*, THE CONSUMERIST (Sept. 16, 2010), http://con.st/10011137.

172. *See* Villarreal, *supra* note 170.

173. CTR. FOR RESPONSIBLE LENDING, *supra* note 162, at 3–4 (finding that almost half of surveyed consumers who reported that they opted out of the default said they did so at least in part to stop receiving overdraft marketing).

174. *See* Laura Northrup, *Opt In to Overdraft Protection Right at the ATM*, THE CONSUMERIST (July 29, 2011), http://con.st/10021347.

175. *See* Laura Northrup, *Chase Now Has Human ATM Greeter Who Helpfully Sells Overdraft Protection*, THE CONSUMERIST (July 14, 2010), http://consumerist.com/2010/07/14/chase-installs-atm-greeter-who-sells-debit-card-overdraft-protection.

176. *Courtesy Pay*, SAN MATEO CREDIT UNION, http://www.smcu.org/accounts/courtesy.php (last visited Aug. 1, 2013).

177. *Sovereign Account Protector*, SOVEREIGN BANK, http://www.sovereignbank.com/personal/promotions/sovereign-account-protector.asp (last visited Aug. 1, 2013).

178. *Bounce Protection*, CENTRAL NATIONAL BANK, https://www.centralnational.com/personal/bounceprotection.asp (last visited Dec. 1, 2013).

179. *See* CTR. FOR RESPONSIBLE LENDING, *supra* note 162, at 6 n.8 (finding this to be a common misconception).

2. Judgment and Decision Biases

Firms that benefit from defaults can harness judgment and decision biases to keep consumers in those defaults. But firms that oppose defaults can defuse these biases or even flip them to push consumers out of the default position.

Institutions faced with the financial information defaults work to ensure that biases support the defaults. For example, one financial institution's opt-out notice appears designed to trigger loss aversion and the endowment effect. It explains:

> [We are] known for [our] exceptional member service. Sharing member information as we have outlined here enables us to maintain this service excellence . . . .
>
> However, federal law also requires that we allow you to opt out . . . . Limiting our ability to share financial information . . . will make it difficult for us to serve you as you might expect.[180]

This reminds consumers that sticking with the defaults will "maintain" the status quo, suggests that the defaults ought to form consumers' expectations (the reference point from which consumers should measure gains and losses), and warns that opting out will cause consumers to lose benefits they now have.[181]

Next, financial institutions encourage procrastination and decision avoidance. The law requires consumers to be given the opportunity to opt out at any time so as to reduce transaction barriers. But institutions may emphasize this fact to encourage procrastination[182]—if a consumer can opt out at any time, she need not take action immediately. Further, although framing rules require the opt-out notices themselves to be "reasonably understandable," institutions can make the opt-out decision appear complex and overwhelming. Some institutions offer a plethora of "privacy policies" that consumers must wade through to understand their opt-out rights.[183]

180. *How to Enable Your Cookies*, *supra* note 164.

181. *See also* Janger & Schwartz, *supra* note 15, at 1243 (discussing specific ways in which financial institutions frame the choice to opt out of the Gramm-Leach-Bliley default as a loss).

182. *Privacy Notice*, CAPITALONE, http://www.capitalone.com/media/doc/corporate/english-privacy-notice.pdf (last visited Aug. 1, 2013) ("You can contact us at any time to limit our sharing.").

183. *Privacy Overview*, METLIFE, https://www.metlife.com/about/privacy-policy/index.html (last visited Nov. 25, 2013) (listing on its "privacy" webpage: an "Online Privacy Policy," a "Customer Privacy Policy," an "Auto & Home Privacy Policy," a "HIPAA Notice

Others surround the required notice with voluminous "explanations" that are difficult to read and understand.[184]

In the face of the overdraft default, on the other hand, banks have waged a marketing campaign designed to negate or reverse the biases that might otherwise give the default traction. Banks have attempted to reposition loss aversion and the endowment effect to encourage opting out using two strategies. One was to pitch opting out prior to the date on which the new legal default rule became effective, thus framing the choice as between keeping an existing endowed position or accepting a change by agreeing to the new default.[185] In their marketing, banks explicitly invoked loss aversion to encourage opting out with copy such as "Don't lose your ATM and Debit Card Overdraft Protection"[186] and asking accountholders whether they wanted to "keep [their] account working the same" or "change [their] account."[187] The other has been to frame opting out not as losing an endowed position but as gaining the bank's overdraft "service" by "opting in."[188]

---

of Privacy Practices for Personal Health Information," as well as a link for "Opting Out of Information Sharing").

184. For example, one institution's webpage accompanying its opt-out notice uses the following, over 100-word sentence:

> However if you do not want us, your financial advisor or your bank, credit union or other financial institution to disclose your personal information to the New Financial Institution, and if you do not want your financial advisor or your bank, credit union or other financial institution to retain copies of your personal information when your financial advisor or your bank, credit union or other financial institution terminates his, her or its relationship with us, you may request that we, your financial advisor and your bank, credit union or other financial institution limit the information that is shared with the New Financial Institution by filling out the Privacy Choices Notice and mailing it to [address].

LPL Privacy Policy and Opt-Out Information, WEBSTER BANK, https://www.webster online.com/personal/products-services/investment-services/LPL-privacy-policy.html (last visited Aug. 1, 2013).

185. *See, e.g.*, Andrew Martin & Ron Lieber, *Banks Apply Pressure to Keep Fees Rolling in*, N.Y. TIMES, Feb. 23, 2010, *available at* http://www.nytimes.com/2010/02/23/your-money/credit-and-debit-cards/23fee.html.

186. *Don't Lose Your ATM & Debit Card Overdraft Protection*, LAPEER COUNTY BANK & TRUST COMPANY, http://www.lcbt.com/2747/mirror/debitcardandatmoverdraftprotection.htm (last visited Aug. 1, 2013).

187. *Stay Protected with Shareplus ATM and Debit Card Overdraft Coverage*, SHAREPLUS FED. BANK, *available at* https://secureforms.c3vault1.com/forms/shareplus/pdf/opt-in-details.pdf (last visited Aug. 1, 2013).

188. *See, e.g.*, Jim Bruene, *Debit Card Overdraft Protection: 2 Steps Forward, 1.9 Back*, NETBANKER (July 13, 2010), http://www.netbanker.com/2010/07/debit_card_overdraft_protection_2_steps_forward_19_back.html (providing graphic from credit union

Second, banks harness choice bracketing and play on discounting to spur opting out. Consumers are given the choice whether to accept overdraft coverage for any and all ATM and debit transactions that might overdraft the account, rather than on a transaction-by-transaction basis.[189] This broad choice bracketing directs consumers' focus to the question of whether they might *ever* need overdraft coverage (e.g., for an emergency), favoring opting out. If instead, consumers were faced with narrow decisions about whether to accept overdraft coverage and fees for particular transactions, consumers could selectively use overdraft for emergencies and decline it for non-emergencies. Broad choice bracketing also makes the benefits of opting out appear immediate and certain and the costs delayed and uncertain. Bank advertising includes themes along the lines of "Privilege Pay works like a safety net for your checking account . . . so you don't get left stranded at a gas station"[190]—thus offering accountholders immediate "peace of mind"[191] that funds will be available in an emergency if the consumer opts out.[192] In contrast, banks downplay the costs of overdrafting, emphasizing that opting out of the default and into the bank's overdraft program is a "free" perk.[193]

Third, rather than allowing procrastination, decision avoidance, and salience and omission biases to lead to inertia, banks place some consumers in a mandated choice scenario and have given others deadlines or encouragement to act. As explained above, some banks require new customers and accountholders attempting to use online banking to opt in or out of overdraft coverage before they can open an account or continue to use online banking. These accountholders are forced to take action and cannot procrastinate or avoid making the decision. For existing accountholders who did not use online banking, bank marketing framed the

that advertises "Opt **In** for Overdraft Coverage on Debit and ATM Cards. . .; CLICK HERE TO OPT **IN**" (emphasis added)).

189. 12 C.F.R. § 205.17 (2014).

190. *Privilege Pay*, FARMERS INSURANCE GROUP FED. CREDIT UNION, https://www.figfcu.com/print.php?id=610 (last visited Aug. 1, 2013).

191. *See, e.g.*, *Stay Protected with Shareplus ATM and Debit Card Overdraft Coverage*, *supra* note 187 ("STAY PROTECTED . . . MAINTAIN PEACE OF MIND"); *Sovereign Account Protector*, *supra* note 177 ("Enjoy the peace of mind of knowing your checks, debits, and payments are automatically honored by setting up an Overdraft Protection Plan.").

192. *Privilege Pay*, *supra* note 190 ("Privilege Pay works like a safety net for your checking account . . . so you don't get left stranded at a gas station . . . .")

193. *See, e.g.*, *Overdraft Protection*, CAPITALONE, http://www.capitalone.com/bank/overdraft-protection/ (last visited Nov. 25, 2013) ("Opting in is free and easy."); *Check Card Overdraft Protection for Your Wescom Checking Account*, WESCOM CREDIT UNION, https://www.wescom.org/accounts/whyoptinoverdraftprotection.asp (last visited Nov. 25, 2013) ("Why Opt in to Check Card Overdraft Protection? It's Free.").

decision as one that must be made immediately or by a certain deadline.[194] Bank marketing also trumpets "It's your choice!,"[195] implying that sticking with the default is not a blameless omission.

Fourth, banks use explicit messaging so that the illusion of control instigates opting out. Bank marketing emphasizes that consumers are "in control" of their overdraft decisions[196] and implies that opting out gives consumers more control than sticking with the default.[197] Because the feeling of control encourages riskier behavior, to the extent that consumers understand that they are taking a risk of incurring overdraft fees, these marketing messages could encourage them to opt out.

3. Preference Formation Effects

As with transaction barriers and biases, the preference-forming effects of defaults can be made stronger or weaker.

Institutions bolster any advice implicit in the financial information defaults with explicit advice to consumers that their privacy is already protected and they need not opt out.[198] Documents and webpages accompanying the financial information default notices commonly emphasize foremost that the institution cares about the consumer's privacy.[199] For example, although a close read of one institution's required notice reveals that the institution shares consumer information to the fullest extent

194. *Urgent Notice Regarding Your Public Service Credit Union Debit/ATM Card*, PUBLIC SERVICE CREDIT UNION, https://www.mypscu.com/docs/odpletteronline.pdf (last visited Aug. 1, 2013) ("Urgent notice regarding your . . . Debit/ATM Card. Your immediate response is needed!"); Bruene, *supra* note 188 (providing graphic from credit union that advertises "August 15 is the deadline to apply if you choose to keep coverage").

195. *See, e.g.*, *Overdraft Protection*, *supra* note 193.

196. *Overdraft Privilege: Stay Protected*, FIRST FIN. BANK, https://www.bankatfirst.com/personal/spending-account-options/overdraft-privilege-opt-in.aspx (last visited Aug. 1, 2013) ("You now control whether or not you want to continue overdraft privilege coverage for ATM withdrawals and everyday check card transactions.").

197. *Overdraft Privilege*, FIRST CMTY. CREDIT UNION, https://www.fccu.org/Resources/PDFs/Overdraft%20Privilege_3_13.pdf (last visited Aug. 1, 2013) ("Keep Your Oversights Under Control"); *Debit Card Overdraft Services*, WEBSTER BANK, https://www.websteronline.com/personal/products-services/checking-services/debit_card_overdraft_services.html (last visited Aug. 1, 2013) ("Giving you control for your everyday debit card purchases.")

198. *See, e.g.*, *Our Privacy Promise to You*, UNITED SERVS. AUTO. ASS'N, https://www.usaa.com/inet/ent_references/CpStaticPages?PAGEID=cp_netprivacy_pub (last visited Aug. 1, 2013) ("If you decide that USAA's rigorous practices meet your privacy expectations, **no further action is required**.").

199. *See, e.g.*, *Wells Fargo Privacy and Security*, WELLS FARGO, https://www.wellsfargo.com/privacy_security/privacy (last visited Aug. 1, 2013) (beginning with "[w]e're committed to protecting your privacy").

permitted by law (i.e., with joint marketing partners, affiliates, and non-affiliates, and for both marketing and non-marketing purposes), the webpage from which this notice can be accessed begins boldly: "SAFEGUARDING YOUR PRIVACY" and continues "[THIS INSTITUTION] TAKES OUR COMMITMENT TO PROTECTING YOUR PRIVACY SERIOUSLY."[200]

Institutions explicitly advise consumers that they will benefit by not opting out. For example, one institution explains that sharing information with affiliates provides customers with the following benefits:

1. Prevention of unauthorized transactions or fraud.
2. Account upgrades with additional benefits.
3. Offers for products and services specifically suited to your individual situation. . . .
4. Increased convenience, making it faster and easier for you to do business with us. . . .
5. Enhanced customer service and responsiveness.[201]

The implication is that consumers who opt out of information sharing will not receive these benefits.

In contrast, banks present the overdraft default in a way that negates the preference-forming effects of defaults. Banks typically present accountholders with two checkboxes, one for "opting in" to the bank's "overdraft protection" and another for "opting out," thus concealing which position is the default.[202] Further, banks advise accountholders that the opt-out position, rather than the default, is in accountholders' best interests, with copy such as "overdraft privilege is designed with you in mind."[203]

Finally, before the overdraft policy default came into effect, banks pressured existing accountholders to opt out of the overdraft policy before they had a chance to experience the new default. Similarly, banks force new customers to make a decision when they open an account. Experience, therefore, does not induce accountholders to choose the default, as they have not had the opportunity to discover that they can manage without purchases

200. *Privacy Protection*, CAPITALONE, http://www.capitalone.com/identity-protection/privacy (last visited Nov. 29, 2013).

201. *Regions Privacy FAQs*, REGIONS, http://www.regions.com/about_regions/all_facts.rf (last visited Aug. 1, 2013).

202. *See, e.g.*, *First Commerce Credit Union Opt-In/Opt-Out Form*, FIRST COMMERCE CREDIT UNION, *available at* http://www.firstcommercecu.org/accounts_resources/consumer_education/new_regulation_over_draft_protection_options_your_action_is_required/opt_in_opt_out_form#form (stating "Please complete this form to Opt-in or Opt-out of overdraft protection" and providing two check boxes, one labeled "OPT-IN" and the other labeled "OPT-OUT").

203. *Overdraft Privilege: Stay Protected*, *supra* note 196.

that would overdraft their accounts or that alternative, cheaper sources of overdraft coverage are available.

C. SUCCESSFUL DEFAULTS

Of course, many default schemes do work as intended. Two well-known examples are the above-mentioned retirement savings auto-enrollment default and the Do Not Call registry.

1. Automatic Enrollment in Retirement Savings Plans

Auto-enrollment allows employers to default employees into participation in defined contribution pension plans.[204] This policy default scheme includes framing rules designed to ensure that the defaults are not too sticky, including a requirement that every employee who is enrolled by default be given regular notices of the right to opt out.[205] These notices must be written at a level that the average employee can understand, so that the opportunity to opt out is not confusing.[206]

Auto-enrollment has been extremely successful in its goal of increasing the number of employees in the default position.[207] As noted above, employers that have made participation in their plans the default have increased their employee participation rates dramatically.[208] The increase has been largest for lower-income consumers, which has been interpreted as evidence that defaults are most helpful for those who need the most help.[209]

204. *Retirement Topics–Automatic Enrollment*, INTERNAL REVENUE SERV., http://www.irs.gov/Retirement-Plans/Plan-Participant,-Employee/Retirement-Topics---Automatic-Enrollment (last visited Aug. 1, 2013).

205. Safe Harbor Requirements, 26 C.F.R. § 1.401(k)-3(d)(2) (2014).

206. *Id.* § 1.401(k)-3(d)(2)(i)(B).

207. However, the default scheme has decreased the average amount individual employees save, contrary to policymaker aims. *See* Ryan Bubb & Richard H. Pildes, *How Behavioral Economics Trims Its Sails and Why*, 127 HARV. L. REV. (forthcoming 2014).

208. *See, e.g.*, Nessmith et al., *supra* note 88, at 6 (comparing enrollment rates for automatic enrollment plans (86%) with voluntary enrollment plans (45%)).

209. *See* John Beshears et al., *Public Policy and Saving for Retirement: The "Autosave" Features of the Pension Protection Act of 2006*, *in* BETTER LIVING THROUGH ECONOMICS 274, 287 (John J. Siegfried ed., 2010) (noting "clear and compelling evidence that automatic enrollment was an effective means of increasing savings and improving economic well-being, particularly of minorities and of the poor"). This interpretation may be erroneous, as there are some low-income employees who participate because of automatic enrollment but for whom participation is not optimal. The details of this argument are beyond the scope of this Article.

2. Do Not Call

Another popular default scheme is the Do Not Call Registry. By default, telemarketers can call people to try to sell to them, but consumers can stop most of these calls by signing up for the Do Not Call Registry. This process is well known, low cost, and easy—consumers can call a toll-free number or register online.[210] Consumers can opt back into the default wholesale by removing their number from the list,[211] or they can provide written explicit consent to selectively opt back into the default and allow a particular firm to telemarket to them.[212] Because this consent must be in writing, the effect is that telemarketers cannot call consumers and orally attempt to convince them to opt back in.

From its inception, the Do Not Call Registry was heavily publicized, and the public responded. Despite having to take some action to opt into the list, consumers placed ten million phone numbers on it in the first four days it was operative,[213] and today over seventy percent of Americans have placed their numbers on the list.[214] Further, it appears that the default sorts consumers reasonably well. On average, those consumers who do not sign up have the least to gain by doing so, because they do not receive many telemarketing calls; those who have much to gain sign up.[215]

---

210. *FTC Approves Two Reports to Congress on the National Do Not Call Registry*, FED. TRADE COMM'N (Jan. 4, 2010), http://www.ftc.gov/opa/2010/01/donotcall.shtm ("[R]esearch has consistently shown widespread public awareness of the program and a steady increase in the number of phone numbers registered."); *see also Register Your Home or Mobile Phone Number*, NAT'L DO NOT CALL REGISTRY, https://www.donotcall.gov/register/reg.aspx (last visited Aug. 5, 2013)(National Do Not Call online registration form).

211. *National Do Not Call Registry*, FED. TRADE COMM'N, http://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry (last visited Aug. 5, 2013).

212. Abusive Telemarketing Acts or Practices, 16 C.F.R. § 310.4 (b)(1)(iii)(B)(*i*) (2014).

213. *Ten Years of Do Not Call*, FED. TRADE COMM'N, http://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry (last visited Aug. 5, 2013).

214. As of 2007, seventy-two percent of Americans had placed their phone numbers on the list. COUNCIL OF ECON. ADVISORS, 2009 ECONOMIC REPORT OF THE PRESIDENT 244 (2009), *available at* http://georgewbush-whitehouse.archives.gov/cea/ERP_2009_Ch9.pdf.

215. *See* Goh Khim-Yong et al., *Consumer Heterogeneity, Privacy, and Personalization: Evidence from the Do-Not-Call Registry* 4–6, 21 (2009), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.216.44 (providing evidence that consumers in more heterogeneous communities more frequently sign up for the Do Not Call list and attributing this to the fact that these consumers receive more telemarketing calls, including more calls marketing goods and services in which they have no interest, because telemarketers cannot target marketing to these consumers as narrowly as consumers living in more homogeneous communities); Goh Khim-Yong et al., *Social Interaction, Observational Learning, and Privacy: The "Do Not Call" Registry* 23–24, 28 (MPRA Working Paper 8225, 2008), *available at* http://mpra.ub.uni-muenchen.de/8225/1/MPRA_paper_8225.pdf (finding that

D. CRACKS IN THE THEORY BEHIND THE USE OF DEFAULTS

The forgoing examples demonstrate that defaults are not always sticky or information-forcing. What drives the rift between defaults in theory and defaults in practice? This Section explains the conditions that drive this rift and draws upon the forgoing examples to reexamine the theories behind the use of defaults in policymaking.

1. Conditions Where Defaults Do Not Work

The key difference between the automatic enrollment retirement saving and Do Not Call default schemes, on the one hand, and the financial information and overdraft defaults, on the other, is the presence of parties that have (1) a strong interest in whether the consumer sticks with or opts out of the default and (2) the ability to shape the presentation of the default and the process for opting out. No party with access to affected employees at the point of the auto-enrollment opt-out decision has a strong interest in pushing consumers in or out of the default. The employers that administer the default do not oppose it, but also do not have a strong reason to try to make it too sticky.[216] The Do Not Call Registry has enemies; telemarketers want consumers in the default position.[217] But telemarketers do not shape the presentation of the Do Not Call list or the process for signing up; that is run entirely by the Federal Trade Commission.[218] Nor do telemarketers have an effective way to reach consumers whose numbers are on the list to lobby or confuse them into selectively opting back in, since consumers must give written, signed consent before a telemarketer can call them.[219]

In contrast, the financial information and overdraft defaults are implemented by the firms that want them to fail. Not all financial institutions

as telemarketing call volume increased in an area, more households signed up for the do-not-call list).

216. Higher participation levels benefit employers because participation increases employee productivity and retention, particularly for those employees whom employers value more. *See* William E. Even & David A. Macpherson, *Benefits and Productivity*, *in* BENEFITS FOR THE WORKPLACE OF THE FUTURE 43, 48–49 (Olivia S. Mitchell et al. eds., 2003). But where the employer provides a matching contribution, higher enrollment can also be costly for the employer.

217. Telemarketers fought the Do Not Call list for years. *See* Mainstream Mktg. Servs., Inc. v. Fed. Trade Comm'n, 358 F.3d 1228, 1233 (10th Cir. 2004) (rejecting telemarketers' First Amendment challenge to the Do Not Call Registry), *cert. denied*, 125 S. Ct. 47 (2004).

218. *See* National Do Not Call Registry, FED. TRADE COMM'N, *available at* https://www.donotcall.gov/faq/faqdefault.aspx (last visited Apr. 13, 2014).

219. *See* Q&A for Telemarketers & Sellers About DNC Provisions in TSR, BUREAU OF CONSUMER PROT., *available at* http://business.ftc.gov/documents/alt129-qa-telemarketers-sellers-about-dnc-provisions-tsr (last visited Apr. 13, 2014).

share customer information with third parties or their affiliates, and not all of those that share with their affiliates allow those affiliates to use the information for marketing purposes. But the institutions that share customer information profit from it and so want their customers to retain their default settings.[220] Not all banks charge overdraft fees, but many that do profit enormously from them and thus have every reason to convince accountholders, and frequent overdrafters in particular, to opt out of the overdraft default.[221] Financial institutions and banks also have access to consumers and use that access to shape the opt-out process and to frame the default at the point of consumer decision. The party opposed to the default is thus able to powerfully influence the consumer's ultimate position.

2. Reexamining the Logic Supporting the Use of Defaults in Policymaking

The failure of the financial information and overdraft defaults to facilitate well-informed consumer choices suggests that the logic underlying the use of policy defaults, penalty defaults, and even altering and framing rules, is flawed. The irony is that while the use of defaults in policymaking is premised on the understanding that irrational biases will make defaults sticky, particularly for poorly-informed consumers, these same biases and this same lack of information may lead defaults to be too sticky, too slippery, or uninformative in many situations.

The theory fails to recognize the degree to which the mechanisms that can make defaults sticky can be manipulated by firms to make those defaults too sticky or even slippery. The very lack of well-formed preferences and a good understanding of available options that facilitates the mechanisms that can make defaults sticky also leaves consumers vulnerable to firm manipulation of those mechanisms. The theory also fails to recognize the depth of the information asymmetry between firms and consumers. A firm facing a penalty default may find it easier to alter the decision environment so as to push consumer biases to favor opting out than to inform and negotiate

220. *See, e.g.*, Rupert Jones, *Barclays to Sell Consumer Data*, GUARDIAN (June 24, 2013), http://www.theguardian.com/business/2013/jun/24/barclays-bank-sell-customer-data ("Bank tells 13 million customers it is to start selling information on their spending habits to other companies."); Catherine New, *Beyond Card Fees: Banks Look to Sell Your Data*, DAILYFINANCE (Oct. 25, 2011), http://www.dailyfinance.com/2011/10/25/beyond-card-fees-banks-look-to-sell-your-data ("[Visa and Mastercard] have plans to sell marketers an analysis of anonymous data that . . . could be used to create targeted online advertising.").

221. *See* PATRICIA CASHMAN ET AL., FED. DEPOSIT INS. CORP., FDIC STUDY OF BANK OVERDRAFT PROGRAMS 56 (2008), *available at* http://www.fdic.gov/bank/analytical/overdraft/FDIC138_Report_Final_v508.pdf (finding that in 2007, overdraft fees amounted to about seventy-five percent of bank deposit account service charges revenue and twenty-five percent of total bank noninterest income).

with the consumer. Most altering and framing rules aim to fine-tune transaction barriers or deliver information. These rules make no attempt to alter the biases and preference formation effects that can make defaults sticky or that can be used by firms to nudge consumers into opting out. Some altering and framing rules may not even alter transaction barriers or be information-forcing. Not all affirmative actions will inhibit opting out—an affirmative mouse click can become reflexive—and not all legally-required notices are read and understood.[222]

Could the financial information and overdraft defaults and their accompanying altering and framing rules be improved? Undoubtedly they could be. But as detailed below, there are limits to altering and framing rules. In the face of strong firm preferences about which position consumers ought to be in, it is possible that even the most carefully crafted default and altering and framing rules would not produce abundant well-informed individual consumer choice.

V. WHY TRACKING DEFAULTS ARE UNLIKELY TO ACHIEVE POLICYMAKERS' GOALS

Currently, transaction barriers, biases, and preference formation effects make the Track-Me position too sticky. Would that change if Track-Me were to become a true policy default, with surrounding altering and framing rules to help those who prefer to opt out to do so? To a degree yes, because some existing transaction barriers would be removed. But biases and preference formation effects would still give a Track-Me default considerable traction, and firms would find ways to erect some transaction barriers without running afoul of altering and framing rules. Moreover, if firms were required to respect a consumer's choice not to be tracked, they would have a stronger incentive to convince consumers not to opt out than they do today. The greater effort firms would expend on keeping consumers in the default could lead fewer consumers to opt out.

What if Don't-Track-Me were the default? Would that lead to consumers sorting themselves into positions that reflect their well-informed preferences? While a Don't-Track-Me setting would require firms to spend significant resources on maneuvering consumers out of the default, firms determined to do so could be successful without necessarily educating many consumers along the way.

This Part suggests strategies that firms could use to keep or put consumers in a Track-Me position, based on strategies firms have used to

222. *See* Ben-Shahar & Schneider, *supra* note 166, at 704–29.

respond to existing defaults. These suggestions are not definitive or exhaustive predictions; firm strategies would necessarily depend on subtle contextual details that cannot be known in advance. But the examples here give the flavor of strategies firms would likely use. This Part then turns to an explanation of why altering rules, framing rules, and competition among firms cannot ensure that tracking defaults will result in informed consumer decisions.

A. HOW FIRMS COULD MAKE TRACKING DEFAULTS FAIL

Even with altering and framing rules intended to encourage consumers to make well-informed decisions that reflect their preferences, firms would have ample opportunities to make these defaults fail. This Section outlines a firm's three main avenues for ensuring the failure of a default: (1) utilizing transaction barriers, (2) harnessing judgment and decision biases, and (3) influencing preference formation effects.

1. Erect, Eliminate, or Invert Transaction Barriers

a) Costs

First, firms would make it easy for consumers to reach the Track-Me position, regardless of the default. For example, when faced with a consumer who has not opted out of a Don't-Track-Me default (or who has opted out of a Track-Me default), a website, program, or device could minimize the costs of opting out by offering the consumer a one-click-opt-out method.

Second, firms would make it costly for consumers to opt into or stay in a Don't-Track-Me position. Although altering and framing rules should lower the costs to consumers who select the Don't-Track-Me position as compared to those costs today, the opt-out process would still be time-consuming because, given current technology, it would need to be performed for every browser on every device and again when new browsers or devices are used. If legally permitted, firms might give coupons and discounts to those who agree to tracking, making it immediately and visibly costly to be in a Don't-Track-Me position.[223] Firms might condition access to content, apps, and other services on consumers being in the Track-Me position, as is the case for many apps and some email services today.[224] When the Netherlands made

223. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1534–35 (2000) (explaining that consumers sell their personal information too cheaply).

224. *See, e.g.*, Adrienne Porter Felt et al., *Android Permissions: User Attention, Comprehension, and Behavior*, *in* SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2012) (discussing conditioning app downloads on permission to track); RT.COM, *supra* note 25 (discussing conditioning Gmail use on permission to scan email content).

Don't-Track-Me the default for websites, most Dutch websites placed "cookie walls" between consumers and website content, pop-up dialog boxes requiring users to accept all cookies to access the websites.[225] As explained above, short of conditioning access on tracking, firms could make refusing to be tracked costly by designing their apps or websites to function poorly when a consumer is in a Don't-Track-Me position.

If the law were to prohibit explicit differential treatment of consumers who did not agree to be tracked, firms might impose more subtle costs instead. For example, firms might inundate consumers with marketing that would only stop if the consumer agreed to be tracked. They might place a complex login process between the website's content and users who are not in a Track-Me position, just as banks require accountholders who have not opted out of the overdraft default to click through a pop-up dialog box to access online banking. Consumers would realize that they can save time by agreeing to be tracked and would soon click "I agree to be tracked" buttons reflexively.[226] The Dutch Parliament found that the cookie walls referenced above led to "mindless clicking of 'I accept' buttons."[227]

Even more subtle costs and perks are possible. For example, rather than contextual advertising (showing consumers ads based on the content the consumer is accessing), firms could show a steady stream of particularly annoying ads (e.g., ads that obscure content, load and play slowly, or contain distracting movement and noise) to anyone who was not in the Track-Me position. In the Netherlands, a few websites now permit access to some content without consumer consent to tracking, but a large pop-up box asking for permission to track remains in the foreground, making it difficult to view the entire site.[228]

---

225. *See, e.g.*, Natali Helberger, *Freedom of Expression and the Dutch Cookie-Wall* 2 (Univ. of Amsterdam – Inst. for Info. Law, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2197251; *Possible Changes to the Privacy Law in the Netherlands,* BIZCOMMUNITY.COM (Feb. 28, 2013), http://www.bizcommunity.com/Article/152/16/89967.html.

226. *Cf.* FTC PRIVACY REPORT, *supra* note 106, at 49 (noting "choice 'fatigue' " problem when web users are repeatedly asked to opt out); Ayres, *supra* note 16, at 2069 (noting the problem that some altering rules are ineffective because people become "habituated to the speed bumps").

227. Helberger, *supra* note 225, at 4. Analysts found that over 90%, and in most cases closer to 99%, of consumers agreed to be tracked when faced with cookie walls on Dutch websites. Bart Schutz, *Can Defaults Save Online Privacy (or "How to Cure a Self-Destructive Law")?*, ONLINEPERSUASION.COM (May 23, 2013), http://www.online-persuasion.com/can-defaults-save-online-privacy-or-how-to-cure-a-self-destructive-law.

228. *See, e.g.*, DE BRAUW, BLACKSTONE, WESTBROEK, http://www.werkenbijdebrauw.nl/ (Dutch website for Dutch law firm) (last visited Nov. 29, 2013); DE

b) Confusion

Firms would have no trouble using confusion to their advantage. Altering and framing rules should combat some of the confusion that exists today, but the default scheme would almost certainly be confusing to many. It likely would consist of a complex mix of Track-Me defaults, Don't-Track-Me defaults, and unalterable Track-Me positions, comparable to financial information and overdraft defaults, which cover some types of information and overdrafts, but not others. Even if altering rules required firms to provide consumers with a simple, easy-to-use opt-out process at the browser or device level, firms would ask consumers to make granular choices about tracking, following the example set by Facebook's notoriously confusing fifty privacy buttons and 170 privacy-setting options.[229]

Firms might also ask consumers to "click here to opt in to our Privacy Policy" to take advantage of consumers who mistake a "privacy policy" for a promise not to share consumer information. If regulators were to prohibit calling a policy that permits tracking a "privacy" policy, firms would find other confusing labels, such as a "Know Your Customer Policy" or a "Personalized Settings Policy." The former sounds like a duty placed on firms and the latter sounds like a benefit designed for consumers, both of which avoid "tracking," a "dirty word" among firms that track consumers today.[230]

c) Futility

Under a true default regime, choosing not to be tracked would be significantly less futile than it is today, because firms would have a stronger legal obligation to respect consumer choices. Yet, consumers likely would not be permitted to avoid all tracking for all purposes; firms would continue to track for "permissible purposes" even those consumers in the Don't-Track-Me position. As with the financial information defaults, consumers might feel that resisting the position preferred by firms is futile.

BRAUW, BLACKSTONE, WESTBROEK, http://www.debrauw.com/ (English website for Dutch law firm) (last visited Nov. 29, 2013).

229. *See* Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES, May 13, 2010, *available at* http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html.

230. *See* Miller & Sengupta, *supra* note 33 (quoting COO of a tracking technology company as saying " 'Tracking is a dirty word' ").

2. Harness Judgment and Decision Biases

a) Salience Effects

The salience of tracking strongly influences most people's privacy-related actions. One experiment found that consumers who are reminded of the privacy implications of disclosure disclose little, but those who are not reminded appear to forget about privacy—many will reveal socially stigmatized and even illegal behavior.[231]

For a Track-Me default, framing rules intended to make the option to opt out "clear and conspicuous" should increase the salience of the default and opt-out choice somewhat, especially if media coverage of a new law about tracking raises consumer awareness. But at the moment consumers could potentially opt out, firms could minimize the salience of this choice. Websites are frequently cluttered with material the user is not interested in, and part of the skill of using the web is learning how to mentally screen out this content. Website design is so flexible that even with reasonably detailed framing rules about font size, positioning, and the like, firms could probably leverage users' skill in screening out information to hide an opt-out option in plain sight.[232] COPPA, for example, requires that privacy policies for children's websites be positioned prominently, yet they are frequently surrounded by other materials that draw users' attention away.[233] One set of lab experiments found that while reminding people about privacy increases privacy-protective behavior, a mere fifteen-second delay between the reminder and the privacy-related decision was enough to negate the effects of the reminder.[234] More blatantly, firms could place content relevant to opting out such that it falls outside the viewing area of small-device screens.[235]

231. Leslie John et al., *Strangers on a Plane*, 37 J. CONSUMER RES. 858, 859–60 (2011).

232. For examples, see *Dark Patterns Library*, Darkpatterns.org, http://darkpatterns.org/ (last visited Nov. 29, 2013) ("A Dark Pattern is a type of user interface that appears to have been carefully crafted to trick users into doing things . . . . Dark Patterns . . . are carefully crafted with a solid understanding of human psychology, and they do not have the user's interests in mind.").

233. *See, e.g.*, JOSEPH TUROW, PRIVACY POLICIES ON CHILDREN'S WEBSITES: DO THEY PLAY BY THE RULES? (Annenberg Public Policy Center Report 2001) (showing how children's websites follow the regulations about the placement of privacy policy links yet are able to surround the links with distracters or otherwise reduce the links' visibility).

234. Idris Adjerid et al., *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency* 8 (unpublished manuscript), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-sleights-privacy.pdf.

235. *See, e.g.*, FTC MOBILE REPORT, *supra* note 106, at 3 ("[W]ith many devices possessing screens of just a few inches, there are practical challenges in terms of how critical information—such as data collection, sharing of information, and use of geolocation data—is conveyed to consumers.").

Even without a planted distraction, at the concrete moment when consumers use an app, website, or device, they are focused on something else, just as a consumer engaging in a financial transaction is attending to the transaction and not the information-sharing implications. Further, any salience brought to a Track-Me default by framing rules would dissipate over time due to "warning fatigue." Even today, few consumers who are given disclosures explaining that apps collect personal information read—and perhaps as few as three percent understand—the app permissions lists.[236]

For a Don't-Track-Me default, firms might interrupt consumer use of apps, websites, or devices with pop-up screens or similar barriers so that consumer focus is diverted to the tracking decision. Alternatively, the same repeated presentation of an "I agree to be tracked" button that would lower the transaction costs of opting out by inducing reflexive clicks could also reduce the salience of the option *not* to opt out, in that consumers clicking mindlessly will not give this option consideration.

b) Omission Bias

Omission bias that favors tracking today would continue to do so under a full-fledged Track-Me default scheme. Given that most consumers are currently in a Track-Me position, firms facing a Track-Me default could encourage the operation of omission bias by emphasizing to consumers that nothing has changed and they need not take any action.

In contrast, firms facing a Don't-Track-Me default would work to overcome the omission bias, perhaps by placing consumers in a forced-choice scenario. Without the option to do nothing, omission bias would not favor the default. Even if framing rules prevented firms from forcing consumers to choose between the default and opting out, firms might borrow from bank marketing materials that state or imply that consumers "must" take action, so that inaction no longer appears to be a blameless omission.

c) Loss Aversion and the Endowment Effect

With respect to Track-Me defaults, firms could work to ensure that loss aversion and the endowment effect continue to favor the Track-Me position. Firms could encourage consumers to treat the default as the reference point against which gains and losses are measured and as the position with which consumers are currently endowed. For example, firms might characterize Track-Me as the position in which websites, devices, or apps work

236. *See* Felt et al., *supra* note 224, § 5.1.

"properly" or "as you have come to expect" and warn consumers that opting out could impair the user experience.

If a Don't-Track-Me default were imposed, firms could frame opting out of the default not as losing an endowed position but as gaining a "personalized" service. Given that a Don't-Track-Me default would be a change from today's Track-Me world, marketing materials might explicitly invoke loss aversion, asking "Would you like to keep" this service "personalized for you?", or "Would you like to change your settings?" Just as banks asked consumers to opt out of the overdraft default before it became operative, firms might ask consumers to agree to tracking while still in the Track-Me position,[237] thus encouraging consumers to view opting out as keeping the status quo. Firms currently tracking consumers might even tailor their campaigns to specific consumers by determining which feature a consumer has used in the past and warning the consumer that she "could" lose that feature if she does not opt out.

d) Procrastination and Decision Avoidance

Firms facing a Track-Me default could nurture procrastination and decision avoidance by reminding consumers that they can "opt out at any time" and suggesting that opting out requires multiple, time-consuming steps. Although altering rules should make the opt-out process easier than it is today, firms would ensure that the process still appears difficult. Even if framing rules required that firms provide consumers with brief, easily-understandable descriptions of the default and opt-out positions, firms might surround these with voluminous impenetrable "explanations."

In contrast, firms facing a Don't-Track-Me default would probably place consumers in a forced-choice scenario so that procrastination and decision avoidance are not options. Firms might also give consumers false deadlines for opting out just as banks did for the overdraft default, to reduce procrastination.

e) Excessive Discounting

As is true today, the time and effort costs of opting out of a Track-Me default, even if small, would be immediate and certain, whereas any benefits would be uncertain and in the future, particularly given that future uses of

237. The W3C preliminary draft explicitly permits this. W3C TPE, *supra* note 104, § 6.3.1 ("Sites MAY ask for an exception, and have it stored, even when the user's general preference is not enabled.").

information are unknowable.[238] To the extent altering rules would permit, firms might impose additional immediate and tangible costs on consumers who opt out of a Track-Me default. Excessive discounting would thus favor the default.

If Don't-Track-Me were the default, firms could make the potential costs of keeping the default seem probable and clear, and promise immediate peace of mind as a benefit of opting out. Imagine a marketing vignette in which a man tries to impress a woman by showing her something on his computer screen, but the woman's attention is drawn to advertising that pops up and implies something embarrassing about him. She reacts negatively and he tries in vain to claim innocence. Advertising copy might then ask "Tired of ads that weren't meant for you? Opt into personalized advertising today." Firms might also downplay the privacy costs of opting out by offering "free" benefits in exchange for opting out. Just as many apps today are "free" but require the consumer to provide their data in exchange, so too a consumer might be asked to opt out of a Don't-Track-Me default in exchange for "free" apps or services.

f) Choice Bracketing

Altering rules accompanying a Track-Me likely would permit consumers to opt out at the browser or device level—a broadly bracketed decision that could lead individuals to make a decision based on the cumulative effect of loss of information privacy, and thus opt out. But firms might ask consumers to opt back into the default "just for this one" firm, website, or app, triggering a narrowly bracketed decision that would favor immediate benefits over privacy concerns.

For a Don't-Track-Me default, firms would not ask consumers to opt out at the browser or device level—that would benefit the firm's competitors as well as the firm—but instead would seek consent to tracking by that particular firm. Each firm would highlight the narrow nature of that opt-out decision.

g) The Illusion of Control

Perceptions of control strongly affect privacy decision making. Consumers who feel more in control of the exchange of their information

238. *See, e.g.*, Acquisti & Grossklags, *supra* note 79, at 6 ("[A]n individual who is facing privacy sensitive scenarios may be uncertain about the values of possible outcomes and their probability of occurrence, and . . . sometimes she may not even be able to form any beliefs about those values and those probabilities."); NEHF, *supra* note 9, at 126–29 (explaining that consumers cannot know how their information will be used or how those uses will affect them in the future).

with firms are more willing to allow those firms to collect more of their personal information.[239] Giving consumers the illusion of more control leads them to both reveal more sensitive information and allow more publication of that information.[240]

Regardless of the tracking default setting, firms could stress to consumers that they are "in control" of their privacy and thus encourage consumers to share more information. For example, Google today suggests that consumers connect their accounts (enabling tracking across accounts) because "[c]onnecting your accounts puts you in control"; it then reminds consumers, "[r]emember, Google won't share your searches or other private information with third-party services without your consent."[241] Google uses information it gathers about consumers without explicit consent, but the "you are in control" pitch deflects attention from this.[242] A legally enforceable default might give consumers a feeling of greater control than they have today, which could lead to less privacy-protective behavior.

h) The Sunk Costs Fallacy

Under either a Track-Me or a Don't-Track-Me default, firms could exploit the sunk costs fallacy to increase the magnetism of the Track-Me position. Rather than placing tracking walls at the start of a consumer's interaction with a device or program, firms might allow consumers to use the device or program, in a limited or temporary fashion, regardless of the consumer's position. Then, once the consumer has sunk costs into learning to use the device or program, the firm could present a tracking wall to prevent further use. This is similar to what happens today with cellphone apps; consumers must select an app and go through most of the download process before they can learn how much data the app will gather from them

239. Nadia Olivero & Peter Lunt, *Privacy Versus Willingness to Disclose in E-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control*, 25 J. ECON. PSYCHOL. 243, 259 (2004); *see also* Stutzman et al., *supra* note 122, at 29 (finding that as Facebook gave users more control over settings that determine which other Facebook users can view their pages, users made more content "private" vis-a-vis other users, but also posted more confidential information, such that Facebook and parties to which it provides data obtained more information about users).

240. Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, SOC. PSYCHOL. & PERSONALITY SCI. 3 (2012).

241. *See* Tate, *supra* note 27 (reporting on "an obscure checkbox on a buried Google account preferences pane, which reads, 'use my Google contact information to suggest accounts from other sites' " and explaining "[b]y default, this box is checked, which means Google has been scanning your Gmail contacts, unless by some miracle you found this option, buried several clicks beyond your Gmail inbox, and disabled it").

242. *Id.*

if they complete the installation process.[243] At that point, the fallacy might incline consumers to agree to tracking, whether that means opting out of a Don't-Track-Me position or back into a Track-Me position.

3. Bolster, Undermine, or Reverse Preference Formation Effects

a) The Endorsement Effect

If a Track-Me default were adopted, firms could channel the implicit advice mechanism to their advantage and reinforce it with explicit advice, along the following lines:

> Most people don't like receiving a lot of advertising for products they don't want and will never buy. That's why Congress decided to make "Know Your Audience" the default for advertising. If you would like to change this setting, you can. But most people prefer to keep the default.

Such scripts would emphasize that the default reflects what most people want and what policymakers have decided that consumers ought to prefer. Firms might also tackle the privacy issue directly and surround any legally mandated disclosure of the right to opt out with assurances that consumers do not need to opt out because the firm "cares" about the consumer's privacy.

In response to a Don't-Track-Me default, firms would likely defuse the implicit advice effect by obscuring which position is the default. Firms might ask consumers to select between "opting in" to the firm's "privacy policy" (where that policy effectively opts the consumer out of the Don't-Track-Me position) or "opting out" (where "opting out" means sticking with the Don't-Track-Me default). Firms could also counter any implicit advice conveyed by a Don't-Track-Me default with explicit advice to opt out.

b) The Experience Effect

For Track-Me defaults, firms would likely emphasize that nothing has changed and the consumer can continue to use the program or device as she has always done. In contrast, firms would likely push consumers to opt out of any Don't-Track-Me position before the position became effective, to avoid the risk that customers might experience the default and develop a preference for it.

* * *

243. *See* Felt et al., *supra* note 224.

Some of the strategies discussed above are at cross-purposes. For example, on the one hand, reminding people that they *control* their own position might encourage risk taking and thus sticking with a Track-Me default. On the other hand, "you are in control" marketing might make salient that consumers are *responsible* for their own positions and thus discourage omission bias that would otherwise favor sticking with a Track-Me default. If a full-fledged tracking default scheme were adopted, firms would gradually refine their marketing by testing a variety of campaigns, using data gleaned from tracking to target their approaches.[244]

B. ALTERING RULES, FRAMING RULES, AND COMPETITION

The analogies between Track-Me and Don't-Track-Me defaults and the existing financial information and overdraft defaults may appear limited in two respects. First, the existing defaults arguably were political compromises, intended to satisfy public clamor for policymaker action without affecting financial institutions' or banks' bottom lines. Perhaps with more political will, altering and framing rules that would facilitate well-informed, unbiased consumer decision making would accompany these defaults. Second, the privacy landscape contains firms—specifically, some web browser and plug-in makers—that are not dependent on revenue generated from tracking. These firms potentially could implement technologies that protect consumer privacy to woo privacy-concerned consumers from doing business with competitors that allow or engage in tracking.

Yet, a legislatively enacted tracking-default scheme is no less likely to be the product of political compromise than the financial-information or overdraft defaults. More fundamentally, as explained further in this Section, no altering and framing rules consonant with the use of defaults in policymaking will be strong enough to neutralize the influence of self-interested firms on consumer behavior. It is likely inherent in the structure of a consumer-choice regime that where consumers have a weak understanding of their preferences and options, firms that have access to consumers and a strong interest in consumers' ultimate positions will shape those positions.

Similarly, financial institutions and banks might compete on the basis that they do not collect consumer financial information and do not provide expensive overdraft coverage, but few do.[245] Competition over privacy

244. *See* Ryan Calo, *Taking Data Seriously: Market Manipulation in the Digital Age*, YALE L. SCH. INFO. SOC'Y PROJECT (Mar. 28, 2013), http://www.yaleisp.org/event/thomson-reuters-speaker-series-ryan-calo.

245. The main exception is the recently launched Bluebird debit card, which is promoted as a way to avoid both overdraft and monthly checking account fees. The card is

appears to be more common, but the effectiveness of this competition is undermined by the limited ability of consumers to understand and assess firms' privacy promises. More importantly, as this Section elaborates, a tracking default scheme might make things worse, because consumers might perceive the law to provide sufficient protection without the help of privacy intermediaries.[246]

1. The Limits of Altering and Framing Rules

Altering and framing rules might seem to easily counter firm ploys to increase or decrease the stickiness or slipperiness of defaults. To make defaults stickier, policymakers might impose costly opt-out procedures. To prevent firms from making defaults too sticky, policymakers might prohibit conditioning transactions on, or giving perks for, sticking with a default. Policymakers might require specified disclosures crafted to frame the default and opt-out positions in ways that harness or defuse biases. Or, policymakers might require disclosures that convey explicit advice about whether consumers ought to stick with the default or opt out. But normative, legal, and practical constraints limit these rules.

a) Respect for Heterogeneous Preferences

There are two assumptions that premise a default regime rather than a mandate for personal-information tracking: first, that consumers have heterogeneous preferences regarding privacy and the benefits tracking can provide, and second, that the law should respect those heterogeneous preferences by allowing consumers to decide for themselves whether to be tracked.

Altering rules that substantially inhibit opting out are inconsistent with respect for heterogeneous individual tracking preferences. For example, reverting defaults that require consumers to opt out every time they open up their browsers or fire up their mobile devices[247] might effectively keep

exempt from the interchange fee restrictions placed on traditional debit cards and its issuer, American Express, makes money from high interchange fees rather than from traditional overdraft and monthly account fees. *See* Andrew Kahr, *Amex's Bluebird Is a No-Fee Checking Account, Not a 'Prepaid Card,'* AMERICAN BANKER (Oct. 16, 2012), http://www.americanbanker.com/bankthink/american-express-bluebird-is-a-no-fee-checking-account-not-a-prepaid-card-1053516-1.html.

246. So too there might be more competition over overdraft fees absent the legal default rule, because some consumers may perceive that the default gives them sufficient control over overdraft fees and they do not need to shop for a bank that does not charge these fees.

247. *Cf.* Paul Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2098–107 (2004) (proposing a default rule that a consumer's personal data cannot be transferred to third parties, complemented by altering rules requiring that the consumer consent to each

consumers in the default position (provided that firms did not manage to make the opt-out process so easy and routine that consumers would opt out mindlessly[248]). But this would be difficult to justify normatively. Although prohibiting differential treatment of consumers depending on whether they have agreed to be tracked[249] could prevent the most blatant ways that firms might maneuver consumers into a Track-Me position, it might also be normatively problematic. Where tracking currently funds the website, app, or device at issue, such a rule could have substantive effects on the availability of these, particularly for consumers who have limited financial means. Such substantive effects may be an appropriate trade-off for increased information privacy, but such effects go beyond providing consumers with choices about tracking.

Framing rules that would be dramatic enough to be effective are also normatively problematic. In a world cluttered with information and decisions, commanding attention requires something more drastic than a neutral description of the default and opt-out positions, such as those currently required for the financial-information defaults. But imagine a mandated disclosure likening tracking to stalking or spying, conveyed through pictures similar to the graphic cigarette warnings recently proposed by the Food and Drug Administration ("FDA").[250] While potentially effective in convincing consumers to stick with a Don't-Track-Me default, this disclosure would be incompatible with the policy goal of allowing people to sort themselves into their desired positions freely, without a strong policymaker push in any particular direction.

Framing rules that require more complex disclosures or other forms of consumer education might be another strategy, one that could in theory reduce consumer preference uncertainty that fuels susceptibility to firm framing manipulations. But in a quickly changing, complex decision

subsequent transfer of her data at the time the data is transferred, with the aim that the default would be sticky).

248. *Cf.* Wang et al., *supra* note 22 ("Some of our participants reported that they began to ignore our nudges after several days. Future work might investigate addressing this habituation effect.").

249. *See* Paul M. Schwartz & Daniel Solove, *Notice & Choice: Implications for Digital Marketing to Youth*, 2ND NPLAN/BMSG MEETING ON DIGITAL MEDIA AND MARKETING TO CHILDREN 4 (2009), *available at* http://digitalads.org/documents/Schwartz_Solove_Notice_Choice_NPLAN_BMSG_memo.pdf (proposing altering rules prohibiting "mak[ing] the provision of access, information, services, or transactions contingent upon a person's" consent to tracking).

250. *See, e.g.*, R.J. Reynolds Tobacco Co. v. Food & Drug Admin., 696 F.3d 1205, 1221–22 (D.C. Cir. 2012) (describing the Food and Drug Administration's proposed cigarette warnings).

environment, the utility of such education is likely to be nil.[251] Only simple, easily actionable messages tend to be effective in public education campaigns.[252] But a policymaker who believes that consumers ought to take a variety of positions with respect to tracking cannot send a simple "just say no" or "just say yes" message.

b) Mis-sorting

A further obstacle to developing more effective altering and framing rules is a practical one—most such rules are unlikely to sort consumers well. Consider an altering rule designed to counter firm manipulation by making it more difficult for a consumer to opt out of a Don't-Track-Me position, such as requiring a consumer to send a signed letter through the U.S. Postal Service.[253] Consumers who are in the habit of using traditional mail would find this altering rule no more than a speed bump, whereas consumers who conduct their lives online are more likely to be impeded by such a rule. Disparate opt-out rates of these two groups then would not reflect underlying preferences about tracking.

Alternately, consider a requirement that consumers pass an online test proving they have an understanding of the default and opt-out positions as a condition of opting out. Although this process might be informative to those who completed it, many consumers dislike being tested and would be deterred from attempting to opt out on this basis. Others have weak reading or comprehension abilities that would impair test performance. Yet consumers who dislike or perform poorly on written tests are not less likely

251. *Cf.* Lauren E. Willis, *Against Financial Literacy Education*, 94 IOWA L. REV. 197 (2008).

252. *See* JESSICA ASCHEMANN-WITZEL ET AL., *Lessons for Public Health Campaigns from Analyzing Commercial Food Marketing Success Factors: A Case Study*, *in* BIOMED CENTRAL PUBLIC HEALTH 9 (2012).

253. *Cf. Long-Term Care HIPAA Notice*, METLIFE, https://www.metlife.com/about/privacy-policy/HIPAA-privacy-policy/long-term-care-notice.html (last visited Nov. 29, 2013):

> You have the right to request a restriction or limitation on Personal Health Information we use or disclose about you for treatment, payment or health care operations, or that we disclose to someone who may be involved in your care or payment for your care, like a family member or friend. . . . To request a restriction, you must make your request in writing to Privacy Coordinator, MetLife, P.O. Box 937, Westport, CT 06881-0937. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply (for example, disclosures to your spouse or parent).

to benefit from opting out than consumers who enjoy and perform well on written tests.

More broadly, any steps that consumers must take to opt out of a default will have differential effects depending on, for example, consumer habits, confidence, technological savvy, and susceptibility to biases. Some consumers might find an opt-out process confusing, while others have no trouble completing it. Similarly, consumers approach choices with different discount functions, and not all consumers are affected by omission bias.[254] Likewise, while most of us are procrastinators, consumers do not all procrastinate on the same things or to the same extent.[255] Heterogeneity in consumer responses to transaction barriers or in consumer biases means altering rules will affect consumers differently, yet this heterogeneity is unlikely to correspond well with consumers' well-informed privacy preferences. Today, for example, tech-savvy consumers are more likely than the average consumer to employ various techniques that prevent tracking, although tech-savvy consumers are no more concerned about privacy generally.[256]

c) Commercial Speech Doctrine Limits

Given the likelihood that firms will engage in marketing that drives judgment and decision biases to favor the Track-Me position, framing rules prohibiting this type of marketing might seem an appropriate response. Policymakers could even require firms to frame the default and opt-out positions in particular ways.

Under current First Amendment doctrine, commercial speech has a substantial degree of protection.[257] Framing rules generally cannot prohibit

254. *See, e.g.*, Christopher F. Chabris et al., *Individual Laboratory-Measured Discount Rates Predict Field Behavior*, 37 J. RISK & UNCERTAINTY 237, 263 (2008) (finding discount functions vary between subjects and correlate with behavior); Jonathan Baron & Ilana Ritov, *Omission Bias, Individual Differences, and Normality*, 94 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 74, 74 (2004) (finding that not everyone is affected by the omission bias, and some even display an action bias).

255. *See, e.g.*, Ernesto Reuben et al., Procrastination and Impatience 16–18 (Jan. 28, 2008) (unpublished manuscript), *available at* http://ssrn.com/abstract=1077708 (finding propensity to procrastinate varies, as does the degree to which people anticipate their own procrastination).

256. *See, e.g.*, RAINIE ET AL., *supra* note 4, at 24 (finding lower-income Internet users report many more problems with the misuse of their personal information, including online stalking and harassment, than higher income consumers); Yong Jin Park, *Digital Literacy and Privacy Online*, 40 COMMC'N RES. 215 (2011) (finding consumers in all socioeconomic groups nearly equally concerned about online privacy).

257. Any governmental restriction on non-misleading commercial speech must (1) directly advance a substantial governmental interest and (2) be narrowly tailored to serve that

firms from using particular speech, graphics, or vignettes to convey commercial messages if those messages are not misleading.[258] Although telling consumers they will not be tracked when they are being tracked is misleading,[259] courts are unlikely to find any of the marketing ploys described above misleading. The government is also limited in the disclosures that it can require firms to make. For example, while a disclosure likening tracking to stalking or spying might be effective in convincing consumers to stick with a Don't-Track-Me default, forcing firms to give such a disclosure might violate current constitutional limits on the regulation of commercial speech.[260]

Without the ability to prevent firm speech that frames the default and opt-out positions or to require disclosures that can reach consumers through dramatic messages, firms have the upper hand; they can better reach the consumer at the point of decision and can frame the decision using anything short of demonstrably misleading speech.

d) The First and Last Mover

Finally, practical limits on regulation will inhibit policymakers' efforts to manipulate consumer judgment and decision biases or to prevent firms from doing so. It is true that firm ploys to keep consumers in Track-Me defaults, move them out of Don't-Track-Me defaults, or move them back into Track-Me defaults will sometimes fall flat or even backfire. Consumers are a diverse and fickle lot; what one consumer finds acceptable another finds out-of-bounds, and a single consumer might find a path-breaking firm's actions disquieting at first but unremarkable if the rest of the market moves in the same direction.[261] However, firms can send a diverse set of marketing messages (informed by behavioral tracking data) and only need one of these to work with any particular consumer. Firms can also experiment with risky

interest. *See* Cent. Hudson Gas & Elec. Corp v. Pub. Serv. Comm'n of New York, 447 U.S. 557, 564 (1980).

258. *See* Willis, *supra* note 34, at 1161 (explaining how current commercial speech doctrine restricts rules prohibiting firm framing manipulations).

259. *See* ScanScout Consent Order, *supra* note 125.

260. *See, e.g.*, R.J. Reynolds Tobacco Co. v. Food & Drug Admin., 696 F.3d 1205, 1221–22 (D.C. Cir. 2012).

261. For example, Google's February 2012 privacy policy allowing third-party data sharing was met with controversy, but few noticed when Microsoft followed suit in October after running the "Scroogled" campaign criticizing Google. *Compare* Jeff Blagdon, *Google's New Controversial Privacy Policy Now in Effect*, VERGE (Mar. 1, 2012), http://www.theverge.com/2012/3/1/2835250/google-unified-privacy-policy-change-take-effect, *with* Edward Wyatt & Nick Wingfield, *As Microsoft Shifts Its Privacy Rules, an Uproar Is Absent*, N.Y. TIMES, Oct. 19, 2012, http://www.nytimes.com/2012/10/20/technology/microsoft-expands-gathering-and-use-of-data-from-web-products.html.

approaches on a small scale or change course quickly if one approach backfires.[262]

Policymakers are not nearly so agile. Policymakers can set framing rules requiring that firms provide consumers with particular disclosures, but firms can run circles around disclosures. Witness the failure of the behavioral-advertising privacy icon today. This simple, universal, and widely-used icon leads to an explanation of how to opt out of receiving behavioral advertising, but while most consumers have received advertising with this icon attached, very few consumers know what the icon means, and even fewer have clicked on it.[263] Policymakers are unlikely to develop any framing rules that present the opportunity to opt out of a default in clearer terms than an icon like this.[264]

Firms are ultimately both the first movers and the last movers and can use these positions to whipsaw default schemes. Firms use marketing to shape consumer perceptions before consumers encounter the opt-out decision and firms then shape the frame at the moment those firms are providing consumers with the legally required opt-out choice. A framing rule can control one aspect of a frame, but firms can place that aspect within a larger frame that determines how effective the legal framing will be. Policymakers can set altering rules, but firms implementing those rules have the final say on how the entire opt-out process is designed. An altering rule does not completely set how the default will be altered; it merely sets one aspect of that process, and firms control the rest. Yet, it is the entire process that affects the stickiness or slipperiness of the default. If the law could

262. *Cf. Facebook Backs Down, Reverses on User Information Policy*, CNN (Feb. 18, 2009), http://www.cnn.com/2009/TECH/02/18/facebook.reversal; *see also* Calo, *supra* note 244.

263. *See* Ur et al., *supra* note 49 (about ten percent of study participants had some idea that the AdChoices icon was related to advertising; none actually knew what it meant or how it functioned); Pedro Giovanni Leo et al., *What Do Online Behavioral Advertising Disclosures Communicate to Users?* (Carnegie Mellon Univ., Working Paper CMU-CyLab-12-008 2012), *available at* http://www.cylab.cmu.edu/research/techreports/2012/tr_cylab12008.html (finding that over half of surveyed consumers believed that clicking on the AdChoices icon would cause more advertising to pop-up and more respondents believed clicking the icon would let them purchase advertisements than understood that the icons had something to do with behavioral advertising); Matthew Creamer, *Despite Digital Privacy Uproar, Consumers Are Not Opting Out*, ADAGE (May 30, 2011), http://adage.com/article/digital/digital-privacy-uproar-consumers-opting/227828 (reporting click-through rate for the AdChoices icon is only .002%–.005%).

264. Mozilla has suggested a system by which websites or apps would present four of a set of eight possible icons that would encapsulate the key features of the privacy practices of the site or app. *See Privacy Icons*, MOZILLAWIKI, https://wiki.mozilla.org/Privacy_Icons (last visited Nov. 29, 2013). This system seems hopelessly complex, given the failure of even a single icon to be well-understood.

respond to each firm maneuver—and then hold everything constant—altering and framing rules might be able to fine-tune the power of a default. But the law cannot require stasis.

2. Will Competition Change the Calculus?

Is it possible that competition could do what government regulation cannot, creating a robust market for privacy, complete with consumers who make well-informed decisions about tracking that reflect their preferences? Some firms already engage in privacy pitches, and one can imagine others: "With our cellphone, no one can track you."; "Google tracks you. We Don't.";[265] "We're a social network, not an advertising network." Firms seeking to compete based on promises not to track consumers would not be limited by the same normative, legal, and practical constraints facing lawmakers. They could unabashedly push the merits of privacy and the demerits of tracking, and they could respond quickly to their competitors' marketing strategies with their own attempts to bend consumer judgment and decision biases in their favor. But will they? And if so, does the default matter?

Although some privacy-based competition has appeared in the marketplace, thus far it appears to be of limited effectiveness. A small cadre of privacy sophisticates may choose websites, apps, and devices based on reliable promises not to track consumers, but most consumers have difficulty distinguishing firms and products on privacy grounds.[266] Competition thus centers on privacy image rather than privacy reality.[267] For example, while the TRUSTe privacy certification seal increases consumer trust in websites,[268]

265. Kunur Patel, *How Do You Brand Consumer Privacy?*, ADAGE (Feb. 13, 2012), http://adage.com/article/digital/brand-consumer-privacy/232694 (quoting advertising copy used by Internet search engine DuckDuckGo).

266. *Cf.* Joseph Bonneau & Sören Preibusch, *The Privacy Jungle: On the Market for Data Protection in Social Networks*, *in* THE 8TH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2009), http://preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle__2009-05-26.pdf (finding that the "economically rational choice for a [social networking] site operator is to make privacy control available to evade criticism from privacy fundamentalists, while hiding the privacy control interface and privacy policy to maximise sign-up numbers and encourage data sharing from the pragmatic majority of users"); Joseph Turow, *Behavior Aside, Consumers Do Want Control of Their Privacy*, ADAGE (Jan. 29, 2013), http://adage.com/article/guest-columnists/behavior-consumers-control-privacy/239376 (demonstrating how firm marketing may convince consumers that they are protecting consumer privacy even when a closer read of privacy policies reveals this protection to be minimal).

267. *See* Patel, *supra* note 265 (describing widespread advertising by web firms, including Google, touting their privacy-protectiveness).

268. Jensen et al., *supra* note 30.

one study found that websites using this seal engage in more privacy-invasive practices than firms without the seal.[269] Microsoft's recent "Scroogled" marketing campaign, which paints Google as a privacy-invader,[270] may turn out to be mere optics. Microsoft's campaign criticizes Google for tracking consumers, but Microsoft also reserves the right to track consumers in the fine print of its contracts.[271] Consumers who realize that privacy marketing is an unreliable indicator of privacy practices may simply assume all firms track them.[272]

A legal default might change this dynamic somewhat, particularly a Don't-Track-Me default that required firms to obtain express consumer consent before tracking. A request for consent would be a conspicuous admission that the firm tracks consumers, which would help consumers distinguish firms based on the firms' tracking practices, a predicate for genuine privacy-based competition.

But because the returns to firms from tracking are only likely to grow,[273] it is likely to be more profitable for most firms to join the firms that engage in tracking rather than compete against them based on privacy. For example, while Apple's Safari web browser blocks third-party cookies, Apple's iPhone tracks users for advertising and other purposes.[274] To the extent that

269. Benjamin Edelman, *Adverse Selection in Online 'Trust' Certifications*, *in* PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE (2009), *available at* http://www.benedelman.org/publications/advsel-trust.pdf.

270. Michael Learmonth, *Microsoft Debuts New Commercials on Privacy, with Google in the Crosshairs; Bringing up Privacy to Draw a Distinction with Rival*, ADAGE (Apr. 22, 2013), http://adage.com/article/digital/microsoft-launches-privacy-tv-campaign-google-crosshairs/241001 (describing Microsoft's use of privacy in its marketing to distinguish itself from Google, and noting that "ad-supported web services are a money-losing side show for Microsoft but a profitable core business for Google"); Geoff Duncan, *Why Do Not Track May Not Protect Anybody's Privacy*, DIGITAL TRENDS (June 9, 2012), http://www.digitaltrends.com/mobile/why-do-not-track-may-not-protect-anybodys-privacy (suggesting that Microsoft set "Do-Not-Track" as the default for IE 10 both as a marketing strategy and to undercut Google's advertising revenue).

271. Strange, *supra* note 39.

272. Tony Vila et al., *Why We Can't Be Bothered to Read Privacy Policies*, *in* ECONOMICS OF INFORMATION SECURITY 143 (L. Jean Camp & Stephen Lewis eds., 2004) (explaining how privacy market functions like a lemons market).

273. *See* James Temple, *Rules Against Online Tracking Don't Go Far Enough*, SAN FRANCISCO CHRON., Mar. 7, 2012, http://www.sfgate.com/business/article/Rules-against-online-tracking-don-t-go-far-enough-3387373.php ("Targeting ads based on search queries, sites visited, stories read and social connections forms the core of the multimillion-dollar business models of many online companies, including Google, Yahoo and Facebook.").

274. *See, e.g.*, Rosa Golijan, *Apple's Tracking Your iPhone Again, but Says You Can 'Limit' It*, NBC.COM (Oct. 12, 2012), http://www.nbcnews.com/technology/apples-tracking-your-iphone-again-says-you-can-limit-it-1C6427715.

consumers understand that the iPhone tracks them, marketing for Safari that stresses the importance of privacy could hurt iPhone sales. Similarly, online retailers might want consumers to stay in a Don't-Track-Me position with respect to geolocational cellphone tracking to prevent their brick-and-mortar competitors from using this tracking to attract market share. However, online retailers are likely to want to use Internet-use tracking for their own purposes. Marketing that encourages consumers to adopt a Don't-Track-Me position for geolocational tracking could imperil marketing efforts to keep consumers in a Track-Me default on the Internet.

Further, the web browser and plugin makers that currently seek to satisfy consumer preferences not to be tracked might fare worse in a world with a legally enforceable Don't-Track-Me option. With the power to opt out of a Track-Me default or stay in a Don't-Track-Me default, consumers might view these intermediaries as no longer necessary to effectuate their privacy preferences.

While it is impossible to know whether a robust privacy market will develop, the "cookie wall" experience in the Netherlands is instructive. Dutch law made plain which firms were tracking consumers online because only those firms had to ask consumers to opt out of the Don't-Track-Me default.[275] But virtually all firms (and even nonprofits[276]) responded to the law by requiring consumers to opt out as a condition of using the firm's website, not by competing on promises not to track.[277]

VI. CONSEQUENCES OF PRIVACY POLICY BY DEFAULT

None of this tells us whether or when Track-Me or Don't-Track-Me is the best position for consumers. Tracking's benefits to society certainly exceed the costs in some situations. But a default scheme surrounded by firm manipulation of consumer biases or confusion to keep consumers in or lead consumers to the Track-Me position creates only the façade of choice. That façade cannot justify the conclusion that Track-Me is the right position. To assess whether and when firms ought to track consumers would require a far more difficult inquiry than checking whether a consumer has clicked a button opting out.[278]

275. Helberger, *supra* note 225.

276. *See, e.g.*, *Cookies*, TUDELFT, http://cookie.tudelft.nl/ (last visited Aug. 1, 2013).

277. *See* Helberger, *supra* note 225.

278. *Cf.* Ayres, *supra* note 16, at 2096 (explaining that where a default and accompanying altering rules do not produce "the appropriate separating equilibrium"—meaning that the right consumers stick with the default and the right consumers opt out—"lawmakers will

Privacy by default seems like an elegant, low-cost way to resolve concerns about personal information tracking without imposing a position on consumers. Leaving tracking decisions to individual consumers also sidesteps difficult tradeoffs between incommensurable values and politically perilous substantive judgment calls that policymakers would rather not make. If all policymakers are aiming for with a notice-and-choice regime of information privacy defaults is to avoid political heat, they may succeed. But if they seek to use tracking defaults as a way to set norms, guide consumers to individually or socially desired positions, or inform consumers through the opt-out decision process, they are likely to fail.

More generally, nudges may not be an effective way to help people make better choices about information privacy. Nudges can be powerful when no one is pushing back. But a push can easily overwhelm a nudge. Existing research supporting such nudges is performed in artificial conditions where firms do not have an opportunity to intervene.[279] But firms can use the same mechanisms and conditions that make nudges work to make nudges fail. Nudges' success in the lab shows that people's privacy decisions are heavily influenced by framing—which, ironically, is also evidence that nudges may not work in practice, given that firms can reframe nudges. For these experiments to inform public policy, researchers must anticipate and account for firms' dynamic responses to the proposed nudges.[280]

Yet, the broader effects of tracking defaults on the politics of information privacy are uncertain. On the one hand, tracking defaults could be a useful, collectively educational, political way-station on the road to better information-privacy regulation. A default makes tracking more visible than it would be were Track-Me the only option. While tracking defaults are unlikely to directly lead individuals to make well-informed decisions, defaults could foment social discussion and debates that would inform the populace.[281] In turn, this could create political pressure for better regulation.

On the other hand, Don't-Track-Me defaults might delay or derail better information-privacy regulation for two reasons. First, by creating the façade

need to face the more traditional decision of whether to suspend freedom of contracting altogether and make the socially-preferred rule mandatory").

279. *See supra* note 22.

280. As described, one set of lab experiments aimed at external validity by briefly redirecting consumers' attention away from a disclosure intended to nudge the consumer to engage in privacy-protective decisions. It found that even a fifteen-second delay was enough to negate the effects of the disclosure. Adjerid et al., *supra* note 234.

281. *Cf.* David Adam Friedman, *Micropaternalism*, 88 TUL. L. REV. 75 *passim* (2013) (making similar argument about supersize soda bans and their impact on discussion and debate about food and health, even if the bans fail in the courts).

of robust choice, courts, commentators, and consumers themselves are more likely to blame consumers for any adverse consequences that might flow from staying in the default position or from opting out. Experience with opting out of the civil justice system is instructive here. Some sellers permit consumers to "opt out" of arbitration and class-action waiver clauses in the fine print of their standard-form consumer contracts (and thus opt back into the default civil justice system) while keeping the good or service.[282] These firms have apparently calculated that the costs resulting from the few consumers who will exercise this choice are well worth the benefits the firms receive. These benefits could include deterring self-blaming consumers from challenging the fine-print clauses, convincing courts that the contracts cannot be unconscionable if consumers can opt out of these clauses,[283] or arguing in the political process that substantive regulation of these clauses is unnecessary because consumers can opt out. So too in the privacy realm, Track-Me defaults with which consumers stick en masse and Don't-Track-Me defaults from which consumers opt out en masse might defuse pressure, whether directly from consumers or through the courts or the political process, for more meaningful reform.

Second, a notice-and-choice regime of defaults not only reflects the current understanding of privacy as an individual choice, but re-inscribes it. The model conveys the message that the problem is one of accommodating heterogeneous consumer privacy preferences or heterogeneous consumer calculi about the right tradeoff to make between their privacy preferences

282. *See, e.g.*, *Discover Gift Cardholder Agreement 2010*, DISCOVER CARD, http://www.discovercard.com/shopcenter/giftcard-terms.shtml (last visited Aug. 1, 2013) ("You may reject this Arbitration of Disputes section but only if we receive a written notice of rejection from you within 30 days of your receipt of the card."); *Comcast Agreement for Residential Services*, COMCAST, http://www.comcast.com/Corporate/Customers/Policies/SubscriberAgreement.html (last visited Aug. 1, 2013) ("IF YOU DO NOT WISH TO BE BOUND BY THIS ARBITRATION PROVISION, YOU MUST NOTIFY COMCAST IN WRITING WITHIN 30 DAYS OF THE DATE THAT YOU FIRST RECEIVE THIS AGREEMENT. . . ."); *T-Mobile Terms & Conditions*, T-MOBILE, http://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions (last visited Aug. 1, 2013) ("YOU MAY CHOOSE TO PURSUE YOUR CLAIM IN COURT AND NOT BY ARBITRATION IF YOU OPT OUT OF THESE ARBITRATION PROCEDURES WITHIN 30 DAYS. . . .").

283. This move has been successful in many courts. *See, e.g.*, Clerk v. ACE Cash Express, Inc., No. 09–05117, 2010 WL 364450 (E.D. Pa. Jan. 29, 2010) (holding class action waiver not unconscionable in part because plaintiff failed to exercise opt-out right); Guadagno v. E*Trade Bank, No. CV 08–03628 SJO (JCX), 2008 WL 5479062 (C.D. Calif. Dec. 29, 2008) (same); Crandall v. AT&T Mobility, LLC, No. 07-750-GPM, 2008 WL 2796752 (S.D. Ill. July 18, 2008) (same); Honig v. Comcast of Georgia, LLC, 537 F. Supp. 2d 1277 (N.D. Ga. Jan. 31, 2007) (holding arbitration clause not unconscionable because consumer failed to exercise opt-out right).

and the value they place on the benefits tracking can provide. Other conceptions of privacy—for example, as a social judgment about when the anonymity required for individual experimentation, reflection, and flourishing necessary for innovation and a liberal democratic society[284] trumps the utility of the free flow of personal information to society[285]—might lead to different policy responses. But it may be that so long as the public understands privacy as a right of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others,"[286] better forms of regulation will remain unimagined.

284. *See, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013) (arguing that privacy is necessary for both innovation and democracy); ALLEN, *supra* note 5; Schwartz, *supra* note 18, at 1647–66.

285. *See* Tene & Polonetsky, *supra* note 6.

286. WESTIN, *supra* note 8, at 7.