Dear IP Scholars Readers,

This Article is too long, and I am in the process of cutting it down. The typical attendee of this conference will be most interested in the two subparts having to do with trademarks and brands, Parts II.C and III.A.2. I will focus my remarks at the conference on these two sections.

Thanks for taking the time to look at this!

Sincerely,

Paul Ohm

# BRANDING PRIVACY

PAUL OHM*

*forthcoming* 97 MINNESOTA LAW REVIEW ____ (2013)

Draft: Please do not cite or quote without permission

*This Article focuses on the problem of the privacy lurch, defined as an abrupt change made to the way a company handles data about individuals. Two prominent examples include Google's decision in early 2012 to tear down the walls that once separated data collected from its different services and Facebook's decisions in 2009 and 2010 to expose more user profile information to the public web by default than it had in the past. Privacy lurches disrupt long-settled user expectations and undermine claims that companies protect privacy by providing notice and choice. They expose users to much more risk to their individual privacy than the users might have anticipated or desired, and they do so long after users stop paying attention to privacy policies. Given the special and significant problems associated with privacy lurches, this Article calls on regulators to seek creative solutions to address them.*

*For new solutions, we should look to trademarks and brands because the information qualities of trademarks can meet the notice deficiencies of a privacy lurch. The novel union of trademark and privacy law yields a new prescription called "branded privacy," which would require every company that handles customer information to associate its trademark with a specified set of core privacy commitments. If a company someday decides to depart from its initial promises—for example, by embracing a new behavioral advertising business model—it may do so, but only under a new name. Under this rule, Facebook would have been allowed to make the switch it made from private to public, but only after it had changed the name of its service to something new, say "Facebook Public" or "Facebook Enhanced." A close elaboration and evaluation of this solution reveals how well it strikes an appropriate balance between robust privacy protection and a dynamic, free market.*

* Associate Professor, University of Colorado Law School. Thanks to the participants of the Privacy Law Scholars Conference and the faculty workshops of the law schools of Florida State University, William & Mary Law School, and the University of Colorado for helpful comments. Thanks specifically to Meg Ambrose, Shawn Bayern, Julie Cohen, Deven Desai, Victor Fleischer, Laura Heymann, Chris Hoofnagle, Jake Linford, Dan Markel, Andrea Matwyshyn, Bill McGeveran, Scott Peppet, and Felix Wu for their thoughts. Thanks also the Michael Wagner for his excellent research assistance.

# INTRODUCTION

We tend to think about how companies threaten individual privacy by examining their data handling policies at frozen moments in time. At a given moment, so the typical reasoning goes, a company may collect too much information about its users, enabling it to compile rich digital dossiers.[1] It may do too little to protect this information, exposing secrets to hackers and unscrupulous employees.[2] It may store information for a much longer time than it has a need to keep it.[3]

This Article reconsiders problems like these within a more dynamic framework, putting frozen moments of time into motion and shifting the focus to the topic of change. What happens when companies rewrite long-established ground rules governing the way they handle data about their users? There is value in studying as a distinct privacy problem the sudden privacy shift, which some have called the "privacy lurch."[4] Users who experience privacy lurches find themselves exposed to distinct harms that policymakers can counter with tailored remedies, solutions which are easy to miss when change is not in focus.

This is a timely subject for study, as significant new privacy lurches have become an increasingly common phenomenon. In March 2012, Google tore down the walls that once separated databases tracking user behavior across its services, letting it correlate for the first time, for example, a user's calendar appointments with her search queries.[5] In 2011, cell phone service providers began experimenting with new uses for the data it had long collected about the physical location of its users.[6] In 2008, broadband cable Internet providers began testing systems that would have allowed them to watch their users' web surfing habits much more than they had in the past, in order to sell targeted advertising.[7]

Privacy lurches like these disrupt long-settled expectations. They foist new ground rules upon millions of users whose attention spans have long since waned. Lurches give lie to the model of the informed user and contradict company claims of meaningful user consent premised on far-fetched theories of the evolving nature of online contracts. They expose to great harm individuals who do not understand the way that the information collected about them has been put to new, invasive uses. They deprive their users the free choice to decide whether the value of a service justifies the tradeoff to personal privacy, particularly when the user feels locked in to a particular provider because of the time and energy he has already invested (think social networks) or the lack of meaningful competition (think broadband Internet service or Internet search).

But despite the many problems with privacy lurches, some might argue we should do nothing to limit them. Privacy lurches are products of a

---

[1] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) [hereinafter SOLOVE, THE DIGITAL PERSON]

[2] Danielle K. Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007).

[3] Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191, 209–15 (2011) (summarizing data retention policies for largest search engines).

[4] James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) [hereinafter Grimmelmann, *Saving Facebook*].

[5] *Infra* Part I.B.1.

[6] *Infra* Part I.B.3.

[7] *Infra* Part I.B.2.

dynamic marketplace for online goods and services.[8] What I call a lurch, the media instead tends to mythologize as a "pivot," a shift in a company's business model celebrated as proof of the nimble, entrepreneurial dynamism that has become a hallmark of our information economy.[9] Before we intervene against the harms of privacy lurches, we need to consider what we might give up in return.

To help balance the advantages of the dynamic marketplace with the harms of privacy lurches, this Article prescribes a new twist on old notice-and-choice solutions. This is admittedly an out-of-fashion approach to information privacy, as many have lost faith in notice and choice.[10] Scholars have described how notice suffers, particularly on the web, from fundamental information-quality problems; we are awash in a sea of lengthy privacy policies that we cannot take the time to read, written by sophisticated parties with an incentive to hide the worst parts.[11]

To breathe a little life back into notice and choice, this Article looks to the trademarks, representing a novel integration of two very important but until now too-rarely connected areas of information law.[12] Trademark laws recognize how certain words and symbols in the marketplace tackle the very same information-quality and consumer-protection concerns that animate

---

[8] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 40 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf ("[A] business may have a legitimate need to change its privacy policy from time to time, especially in the dynamic online marketplace.") [hereinafter FTC, ONLINE BEHAVIORAL ADVERTISING].

[9] *Infra* Part I.A.

[10] *E.g.* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 821–28 (2000) (critiquing arguments for privacy as control); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1392–1402 (2000) (critiquing arguments for privacy as choice). *See also* N.Y. Times Editors, *An Interview with David Vladeck of the F.T.C.*, MEDIA DECODER BLOG (Aug. 5, 2009, 2:24 PM) http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/ (describing search for new framework for protecting privacy beyond notice and choice by new head of the FTC's Bureau of Consumer Protection).

[11] *E.g.* Ryan Calo, *Against Notice Skepticism*, 87 NOTRE DAME L. REV. ___ at 121–23 (forthcoming 2012), *available online at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1790144; Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES AND PRACTICES 363 (Alessandro Acquisti et al. eds., 2007).

[12] Scholars have compared online privacy to different aspects of the broader field of unfair competition law, within which trademark law is situated. Many, for example, have written about the common law right of publicity, which straddles the two areas. *E.g.* Laura Heymann, *The Law of Reputation and the Interest of the Audience*, 52 B.C. L. REV. 1341 (2011); Stacey L. Dogan, *What the Right of Publicity Can Learn from Trademark Law*, 58 STAN. L. REV. 1161 (2006). Others have noted how particular trademark or unfair competition remedies may impinge on personal privacy or vice-versa. *E.g.* Alberto J. Cerda Silva, *Enforcing Intellectual Property Rights by Diminishing Privacy: How the Anti-Counterfeiting Trade Agreement Jeopardizes the Right to Privacy*, 26 AM. U. INT'L L. REV. 601 (2011). Still others have looked at particular developments that have put pressure on both trademark and privacy law. *E.g.* William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105 (2009); James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1 (2007). But none of these articles analyze the ways in which the theoretical underpinnings of trademark law can be used as a tool to correct the fundamental flaws in notice-and-choice solutions, the most prominent tools used to ensure privacy.

notice-and-choice debates in privacy law. Scholars who study marketing, branding, and trademark theory describe the unique informational power of trademarks (and service marks and, more generally, brands) to signal quality and goodwill to consumers concisely and unambiguously.[13] Trademark scholars describe how brands can serve to punish and warn, helping consumers recognize a company with a track record of shoddy practices or weak attention to consumer protection.[14]

This Article proposes that we use these well-known information qualities of trademarks to meet the notice deficiencies of privacy law. It recommends that lawmakers and regulators force almost every company that handles customer information to bind its brand name to a fully specified set of core privacy commitments.[15] The name, "Facebook," for example, should be inextricably bound to that company's specific, fundamental promises about the amount of information it collects and the uses to which it puts that information. If the company chooses someday to depart from these initial core privacy commitments, it must choose a new name to describe its modified service, albeit perhaps one associated with the old name, such as "Facebook Plus" or "Facebook Enhanced."

Although this "branded privacy" solution is novel, it is well-supported by the theoretical underpinnings of both privacy law and branding theory. It builds on the work of privacy scholars who have looked to consumer protection law for guidance.[16] Just as companies selling inherently dangerous products are obligated to attach warning labels,[17] so too should this obligation extend to companies shifting privacy practices in inherently dangerous, expectation-defeating ways.[18] And the spot at the top of every Internet web page displaying the brand name is arguably the only space available for an effective warning label online.

Branded privacy finds little direct support from traditional trademark theory, which focuses almost exclusively on the source-identifying role of trademarks, but it is well supported by other, more ancillary aspects of trademark theory and doctrine, which emphasize the connection between trademarks and quality control. It finds even stronger support from the recent work of a group of scholars—who have not never before been identified as a separate scholarly "movement," and whom I am giving the moniker, "the New Trademark" scholars—who urge lawmakers to find ways to reconceptualize trademarks as swords used on behalf of consumers rather than shields used to defend producers.[19]

At the same time, because this solution focuses on fixing information-quality problems during privacy lurches rather than prohibiting them outright, and by restricting mandatory rebranding only to situations involving a narrow class of privacy promises, it leaves room for market actors to innovate, striking a nice balance between the positive aspects of dynamism and the negative harms of privacy lurches. Companies will be free to evolve and

---

[13] Barton Beebe, *The Semiotic Analysis of Trademark Law*, 51 UCLA L. REV. 621 (2004).

[14] Note, *Badwill*, 116 HARV. L. REV. 1845 (2003).

[15] "Almost" because a few carve outs are recommended for very new companies still actively experimenting with business models. *Infra* Part III.E.

[16] James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L.J. 793 (2010) [hereinafter Grimmelmann, *Product Safety*].

[17] *Infra* Part II.B.1.

[18] *See* Grimmelmann, *Saving Facebook, supra* note 4, at 1202 ("[Beacon] made both Facebook and its partner sites unreasonably dangerous services.").

[19] *Infra* Part III.A.2.(c).

adapt their practices in any way that does not tread upon their core privacy commitments, but they could abandon a core commitment only by changing their brand. This rule will act like a brake, forcing companies to stop and engage in internal deliberation about the class of choices consumers care about most, without preventing dynamism when it is unrelated to those choices. And when companies do choose to modify a core privacy commitment, their new brands will send clear, unambiguous signals to consumers and privacy watchdogs that something important has changed.

The Article proceeds in three parts. Part I describes the problem with privacy lurches, giving examples of recent lurches and elaborating the special harms (and risks of harm) that privacy lurches cause. Part II outlines what must be done to deal with the problem of privacy lurches, identifying the shortcomings of solutions proposed by others, and embracing notice-and-choice solutions that improve the information-quality problems that plague most alternatives. This Part then shows how theories of trademark and brands have treated very similar information-quality problems. Finally, Part III develops the branded privacy solution, explains its virtues, offers variations to strengthen or weaken its effects as situations demand, discusses what legal reforms are needed to implement the idea, and responds to anticipated critiques.

# I. PIVOTS AND PRIVACY LURCHES

## A. The Pivot

We begin by taking on what may soon be regarded as a sacred cow, the "pivot." Although the word and the idea probably pre-date the use by entrepreneur Eric Ries, they are most often associated with him, his blog,[20] and his book, *The Lean Startup*.[21] Ries defines a pivot as "the idea that successful startups change directions but stay grounded in what they've learned."[22] Pivots have happened for as long as we have had companies, but both their incidence and their importance have increased as business models shift to the Internet, which itself changes so quickly as to obsolete business models before a company gets off the ground.[23]

Pivots have become part of a new dynamic marketplace for online services. In this new world, a start-up that fails brings no shame to its founders and investors, so long as it "fail[s] gracefully."[24] Ries himself argues that "[f]ailure is a prerequisite to learning."[25] Software pioneer Mitch Kapor estimates that "roughly 15 to 20 percent" of the companies he funds through his start-up investment fund "have gone through radical transformations."[26]

In fact, the pivot has been valorized as a sign that founders are trying to harness the engine of creative destruction.[27] Many bloggers and writers in the trade press recite with great admiration the now-enormous companies

[20] STARTUP LESSONS LEARNED BLOG, http://www.startuplessonslearned.com/.
[21] ERIC RIES, THE LEAN STARTUP (2011).
[22] Eric Ries, *Pivot, Don't Jump to a New Vision*, STARTUP LESSONS LEARNED BLOG, June 22, 2009, http://www.startuplessonslearned.com/2009/06/pivot-dont-jump-to-new-vision.html.
[23] Jenna Wortham, *In Tech, Starting Up by Failing*, N.Y. TIMES, Jan. 18, 2012, at B1.
[24] *Id. Also* Steve Lohr, *With a Leaner Model, Start-Ups Reach Further Afield*, N.Y. TIMES, Dec. 6, 2011, at D3.
[25] RIES, *supra* note 21.
[26] Wortham, *supra* note 23.
[27] *See* JOSEPH SCHUMPETER, CAPITALISM, SOCIALISM AND DEMOCRACY (1942).

that once pivoted: Flickr "started out as a feature of an online game" and PayPal "was focused on the idea of beaming money between hand-held digital assistants."[28] The customer-facing music recommendation service Pandora started as a service aimed at businesses like AOL and Yahoo.[29]

Pivots are seen as a continuation of the dot-com-boom-era maxim that sophisticated investors invest in people and not their ideas.[30] The difference today, according to pivot proponents, is the falling cost of starting an online business.[31] This has given rise to "a remarkable increase in the degree of entrepreneurial experimentation."[32]

As a key component of the success of tech startups in Silicon Valley, the pivot thus becomes a central part of the operation of our entire economy. The Obama Administration touts entrepreneurs whenever it discusses its agenda for strengthening the economy and creating jobs.[33] The administration launched a broad initiative it calls "Startup America," intended to "celebrate, inspire, and accelerate high-growth entrepreneurship throughout the nation."[34] Republican candidates seeking to replace the President talk a lot about start-up entrepreneurship on the campaign trail as well.[35] Pivots fuel entrepreneurship, which seems to be the only engine of the economy that still functions properly. Who could possibly say anything bad about them?

## B. Privacy Lurches

But we should pause from celebrating nimble pivots and corporate dynamism to consider some of their costs, and in particular, costs to privacy. Companies that pivot after amassing large databases full of information about individual users too often choose to use the information in new ways, reneging on express and implied promises made when those users first signed up. Often these pivots fit under the subcategory of "monetization" strategies, which is merely code for ways to convert user secrets into cash.[36] These "privacy lurches" can be deeply disruptive to settled expectations and often leave users feeling trapped between bad choices: tolerate significantly less privacy or abandon a service in which they have invested time, energy, and social effort. The next subpart will argue that privacy lurches are significant

---

[28] *Id.*

[29] Tom Grasty, *The Difference Between a 'Pivot' and a 'Reboot'*, IDEA LAB, Feb. 22, 2012, http://www.pbs.org/idealab/2012/02/the-difference-between-a-pivot-and-a-reboot048.html.

[30] *The Pivotal Moment*, THE ECONOMIST, Dec. 2, 2010, http://www.economist.com/node/17633101.

[31] *Id.*

[32] *Id.* (quoting Bill Sahlman of Harvard Business School).

[33] http://www.whitehouse.gov/startup-america-fact-sheet.

[34] *Id.*

[35] Mitt Romney's Florida Republican Primary Speech, Jan. 31, 2012, *available at* http://www.washingtonpost.com/blogs/election-2012/post/mitt-romneys-florida-republican-primary-speech-full-text/2012/01/31/gIQA8tYKgQ_blog.html ("My vision for free enterprise is to return entrepreneurship to the genius and creativity of the American people. . . . I will make America the most attractive place in the world for entrepreneurs, for innovators, and for job creators.").

[36] Martin Zwilling, *Top 10 Ways Entrepreneurs Pivot a Lean Startup*, FORBES (Sept. 16, 2011, 12:01 AM), http://www.forbes.com/sites/martinzwilling/2011/09/16/top-10-ways-entrepreneurs-pivot-a-lean-startup/ (listing ten types of pivots including, at number seven, the "value capture pivot," referring to the "monetization or revenue model).

and special privacy problems that deserve tailored solutions. But first, consider four prominent recent examples.

1. Google's 2012 Privacy Policy Transformation

In January 2012, Google announced it was making significant changes to its many privacy policies.[37] Most importantly, it consolidated most of the "more than 70" privacy policies it had previously scattered across its various products into a single, omnibus privacy policy.[38]

The announcement inspired a deluge of commentary, much of it critical but some supportive.[39] Many observers focused on the most important substantive shift announced, that Google would begin combining data about its users across services that historically it had kept separate.[40] The company described this change as a boon for users, praising "the cool things Google can do when we combine information across products."[41] As an example, it crowed that "[w]e can provide reminders that you're going to be late for a meeting based on your location, your calendar and an understanding of what the traffic is like that day. Or ensure that our spelling suggestions, even for your friends' names, are accurate because you've typed them before."[42]

Some were less enthused. The Center for Digital Democracy, a consumer protection and privacy non-profit, charged Google with "a failure to be candid with users," and for violating a consent decree it had entered into with the Federal Trade Commission (FTC) in 2011 promising reformed privacy practices.[43] Similarly, the Electronic Privacy Information Center (EPIC) sued the FTC in federal court to compel the agency to block the consolidation of user data, accusing the FTC of "placing the privacy interests of literally hundreds of millions Internet [sic] users at grave risk" by failing to act.[44] A judge dismissed the suit as an attack on a non-reviewable agency action, but only after expressing the opinion that the complaint "advanced serious concerns that may well be legitimate."[45]

Regulators expressed similar concerns. Eight members of the House of Representatives sent Google executives a request for more information.[46]

---

[37] Alma Whitten, *Updating Our Privacy Policies and Terms of Service*, THE OFFICIAL GOOGLE BLOG (Jan. 24, 2012, 2:30 PM), http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

[38] *Id.*

[39] Jon Brodkin, *Google Privacy Change Taking Effect Today is Illegal, EU Officials Say*, ARS TECHNICA (Mar. 1, 2012, 11:45 AM), http://arstechnica.com/tech-policy/news/2012/03/google-privacy-change-taking-effect-today-is-illegal-eu-officials-say.ars (summarizing concerns by regulators and privacy activists).

[40] *Id.*

[41] Whitten, *supra* note 37.

[42] *Id.*

[43] Demedia, *FTC Should Halt Google Privacy Changes, as Violation of Consent Decree*, CTR. FOR DIGITAL DEMOCRACY (Feb. 10, 2012, 3:31 PM), http://www.democraticmedia.org/ftc-should-halt-google-privacy-changes-violation-consent-decree.

[44] Complaint ¶ 12, Elec. Privacy Info. Ctr. v. FTC, 2012 WL 413966 (D.D.C. Feb. 8, 2012) (No. 1:12-cv-00206).

[45] Memorandum Opinion at 11, Elec. Privacy Info. Ctr. v. FTC, No. 1:12-cv-00206 (D.D.C. Feb. 24, 2012), *available at* https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2012cv0206-12.

[46] Letter from Congressman Ed Markey et al. to Larry Page, CEO, Google (January 26, 2012), *available online* at http://markey.house.gov/sites/markey.house.gov/files/documents/2012_0126.Google%20Prviacy%20Letter.pdf.

One of the most vocal was Representative Ed Markey, who released a statement complaining that "[s]haring users' personal information across its products may make good business sense for Google, but it undermines privacy safeguards for consumers."[47] State officials, through the National Association of Attorneys General, sent a letter focusing on the lack of an opportunity to opt out of the pooling of data.[48]

European regulators concurred. Several national data-protection authorities from countries across Europe asked Google to delay implementing its planned changes.[49] At the same time, they asked one of their ranks, the French regulator CNIL, to open an investigation into the shift.[50]

2. NebuAd and Phorm

When telephone and cable television companies began providing broadband Internet service at the end of the 1990's, they embraced a straightforward fee-for-access business model, charging subscribers a monthly fee to be connected to all online services.[51] Under this business model, the broadband providers had no incentive to intrude into subscriber privacy, and they restricted their scrutiny of customer behavior to very limited circumstances involving the protection of the security of their networks.[52]

New economic pressures in the first decade of the twenty-first century began to tempt these providers to redefine their customer privacy policies. Data-hungry applications like streaming video and voice telephony spurred users to demand more networking bandwidth, which required costly infrastructure upgrades.[53] Providers also eyed jealously Google's ascension, which was based almost entirely on sales of advertising tied contextually to a user's online behavior.[54] Feeling pressure to find new sources of revenue, these providers began to be approached, in 2008, by new companies touting new technologies for trading user secrets for cash.[55]

Two companies in particular, NebuAd and Phorm, asked providers to install systems that could peer, at least a little, into the web surfing habits of their subscribers, taking advantage of deep packet inspection technology.[56] The NebuAd and Phorm systems would know, for example, that subscriber A frequented travel websites while subscriber B bought shoes online.[57] These profiles could then be sold to advertisers, who would deliver ads directly to a user's desktop, again using NebuAd and Phorm technologies.[58]

---

[47] Katy Bachman, *Pols to Google: Wrong Answers Lawmakers Want More Detail from Search Giant About New Privacy Policy*, ADWEEK (Jan. 31, 2012), *available at* http://www.adweek.com/news/technology/pols-google-wrong-answers-13791.

[48] Nat'l Ass'n of Attorneys Gen., *Attorneys General Express Concerns Over Google's Privacy Policy*, NAAG.ORG (Feb. 22, 2012), http://www.naag.org/attorneys-general-express-concerns-over-googles-privacy-policy-attorneys-general-express-concerns-over-googles-privacy-policy.php.

[49] James Kanter, *E.U. Presses Google to Delay Privacy Policy Changes*, N.Y. TIMES, Feb. 3, 2012, at B3.

[50] *Id.*

[51] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417 (2009) [hereinafter Ohm, *Rise and Fall*].

[52] *Id.* at 1465–68.

[53] *Id.*

[54] *Id.* at 1426.

[55] *Id.*

[56] *Id.* at 1437.

[57] *Id.*

[58] *Id.*

Phorm focused most of its attention on providers in the UK, while NebuAd concentrated on the U.S. market, but in both countries, the responses were the same: fear, outrage, and regulatory scrutiny.[59] The UK's Information Commissioner strongly hinted that Phorm should offer the service only on an opt-in basis.[60] U.S. congressmen held numerous hearings and wrote letters to broadband providers (mostly cable operators) who had entered into contracts with NebuAd.[61] State Attorneys General conducted parallel investigations.[62] In the end, NebuAd's and Phorm's provider partners began to abandon them. Today, NebuAd no longer exists, and Phorm has scaled back its ambitions greatly.[63]

3. Cell Phone Location Privacy

If 2008 was the year to worry about deep packet inspection, then 2011 was the year to worry about cell phone location privacy.[64] During 2008, newspapers worldwide ran stories about how cell phones were being used to track the physical locations of customers. Among the most sensational were stories relating to two events, one involving a German legislator and another involving the Apple iPhone.

German politician Malte Spitz obtained court permission to access the records of his location kept by his provider, Deutsche Telekom.[65] Spitz shared the data with the Die Zeit newspaper, which produced online graphics tracing Spitz's movements over a six month period at a startling degree of granularity.[66] On an almost hour-by-hour basis, Die Zeit's visualizations show Spitz's location, movements, and incoming and outgoing phone calls.[67]

About a month later, computer researchers Alasdair Allan and Pete Warden revealed that Apple's iPhones contain a hidden file that stores a historical record of where the device has been carried.[68] Although the locations in these files tend to be imprecise and sometimes a little inaccurate, they can still be used to construct a fairly faithful historical trail of movement.[69] Within days, the Wall Street Journal reported that both iPhone and

---

[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] Brodkin, *supra* note 39; Glyn Moody, *Phorm Still Looking for a Large-Scale Deployment, Still Finding Investors*, TECH DIRT (Nov. 4, 2011, 2:42 PM), http://www.techdirt.com/articles/20111103/10133616623/phorm-still-looking-large-scale-deployment-still-finding-investors.shtml.
[64] Jason Ankeny, *Year in Review 2011: Lawmakers and Consumers Anguish Over Mobile Data Security*, FIERCE MOBILE CONTENT (Dec. 21, 2011, 2:33 PM), http://www.fiercemobilecontent.com/special-reports/year-review-2011-trends-shaped-mobile-content/year-review-2011-lawmakers-and-consume.
[65] Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know It*, N.Y. TIMES, March 26, 2011, at A1.
[66] *Tell-All Telephone*, ZEIT ONLINE, http://www.zeit.de/datenschutz/malte-spitz-data-retention (last visited September 24, 2011).
[67] *Id.*
[68] Alasdair Allan, *Got an iPhone or 3G iPad? Apple is Recording Your Moves*, O'REILLY RADAR BLOG (April 20, 2011), http://radar.oreilly.com/2011/04/apple-location-tracking.html.
[69] *Cf.* House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, *Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services*, June 24, 2010 at 10 (Testimony of Professor Matt Blaze), *available at* http://www.crypto.com/papers/blaze-judiciary-20100624.pdf

Android phones not only store location information but also send that information back to Apple and Google respectively.[70]

Several Congressional committees launched probes into the matter and spent the spring and summer holding hearings and trading letters with Apple, Google, and other companies related to smartphone industries.[71] Congressional scrutiny has not let up, and at the time this Article was written, at least four bills have been introduced in the current Congress that would regulate cell phone tracking.[72]

Although almost everybody seems to agree that mobile location privacy is becoming an important problem, the debate so far has failed to capture the diversity and complexity of different problems that confusingly sit under the single umbrella of mobile privacy. Some of these problems involve privacy lurches but others do not. First, there are the two problems discussed above, cell phone service providers tracking cell tower registration information (used to track Malte Spitz) and cell phone software developers tracking this same data (Apple and Google). Second, we can add a host of other privacy threats, from cell phone hardware manufacturers (like Nokia or Research-in-Motion) to app developers (Yelp or Google Maps) to services accessible by phone (FourSquare and Loopt), all of which receive location information, some with meaningful consent, some without.

Of the problems listed above, a few are not privacy lurches, as I have defined them. FourSquare and Loopt, for example, are relatively new companies that launched with an aggressively anti-privacy business model revealed to consumers from the start.[73] To participate in either service, one must give up some privacy in location, and because of the way the tools are marketed and designed, this sacrifice should come as no surprise to users.[74]

But most of the other examples given are at least arguably privacy lurches. Cell phone providers and manufacturers, for example, have collected cell tower information for decades, but only recently have they been tempted to monetize this information.[75] And although Apple and Google have been in

(describing how cell tower registration information can be used to track location "with a level of accuracy that can approach that of GPS").

[70] Julia Angwin & Jennifer Valentino-DeVries, *Apple, Google Collect User Data*, WALL ST. J. (April 22, 2011, 1:58 PM), http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

[71] Tanzina Vega, *Congress Hears from Apple and Google on Privacy*, N.Y. TIMES (May 10, 2011, 2:36 PM), http://mediadecoder.blogs.nytimes.com/2011/05/10/congress-hears-from-apple-and-google-on-privacy/.

[72] Geolocation Privacy and Surveillance ("GPS") Act, S.1212, 112th Cong. (2011); Location Privacy Protection Act of 2011, S.1223, 112th Cong. (2011); Commercial Privacy Bill of Rights Act, S.799, 112th Cong. (2011); Electronic Communications Privacy Act Amendments Act of 2011, S.1011, 112th Cong. (2011).

[73] Jason Stamper, *Foursquare, Gowalla, Brightkite, Loopt: A Stalker's Dream?*, CBRONLINE.COM (June 15, 2010).

[74] This is not to say that these services represent no threat to privacy. On the contrary, they may threaten privacy in ways their users do not understand—for example, by making their travels around town available to a police officer with a browser or a subpoena—but that kind of problem is beyond the scope of this Article.

[75] Tom Simonite, *Mobile Data: A Gold Mine for TelCos*, TECHNOLOGY REV., May 27, 2010, http://www.technologyreview.com/communications/25396 ("Cell phone companies are finding that they're sitting on a gold mine—in the form of the call records of their subscribers.").

the cell-phone operating system business for only a few years each, neither one was known to have been collecting this information until very recently.[76]

4. A Slow-Moving Lurch: Facebook's Shift from Private to Public

The hallmark of the lurches described so far is the suddenness of the large shift. In every case, a long-established incumbent player with millions of customers (and in almost every example, with a significant market share) instituted a dramatic change in the way it handled user information, virtually overnight. Another very important privacy lurch has happened much more slowly, although for that reason calling it a lurch does some violence to language. Facebook has steadily, slowly transformed itself from a very private social network into a nearly public one.

Although we can measure where Facebook falls along a continuum of private to public in many ways, using many metrics, consider one especially important measure: the degree of accessibility of the facts that Facebook users submit to people other than "Friends" and "Friends of Friends." In other words, how much can Facebook user A, who is not part of Facebook user B's extended social network, know about B? And even more importantly, how much can a non-Facebook user know about people using Facebook?

As anybody who has seen the movie knows, Facebook began as an exclusive service.[77] Only college students at certain elite colleges were given access to the network, and people on the outside had almost no visibility to what was happening inside.[78] But over time, Facebook has tried to invert itself, switching from a mostly private to a mostly public service.[79] Consider the information found on the Facebook profile page—picture, gender, city, personal interests. In the beginning, none of this information was available outside the network by default.[80] Most importantly, this meant that Google's search engine spider could not harvest information about Facebook users, meaning search queries for names never returned Facebook results.[81]

In July 2009, perhaps to compete with Twitter, a service that has been intrinsically public from birth,[82] Facebook flipped the default, making what the company called "Basic Info"—photo, gender, hometown, current city, and biography—for the first time visible to the world at large.[83] Users could opt out of sharing some of these pieces of basic info, by navigating Facebook's famously complex privacy settings. But many fields—including

---

[76] This last example demonstrates how a lurch can occur even if practices do not change. Apple has probably collected location information since it first shipped the iPhone. But because the particular privacy invasion was unknown to consumers until recently, it represents a lurch in expectations. Granted, this kind of lurch may not be as remediable as shifts away from binding contracts. *See infra* Part III.C.

[77] THE SOCIAL NETWORK (Columbia Pictures 2010).

[78] Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, EFF DEEPLINKS BLOG (April 2010), http://www.eff.org/deeplinks/2010/04/facebook-timeline.

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] Chad Skelton, *New Facebook Privacy Settings Make Your Private Photos Public*, THE VANCOUVER SUN (Dec. 10, 2009, 8:59 AM), http://communities.canada.com/vancouversun/blogs/parenting/archive/2009/12/10/facebook-privacy-settings-profile.aspx (speculating changes were made to compete with Twitter).

[83] Chris Kelly, *Improving Sharing Through Control, Simplicity, and Connection*, THE FACEBOOK BLOG (July 1, 2009, 12:11 PM), http://blog.facebook.com/blog.php?post=101470352130.

name, picture, city, gender, networks, and fan pages—were no longer subject to hiding.[84]

Pulling back the lens a bit, the major shift in 2009 constituted but a single step in a much longer series transforming Facebook from a private to a public service. Facebook has instantiated its policies in software but revealed them in its written privacy policies, allowing commentators to marks their evolution. Kurt Opsahl of the Electronic Frontier Foundation summarized this trend in a blog post, comparing six successive versions of the document.[85] In 2005, the privacy policy promised that

> No personal information that you submit to Thefacebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings.[86]

By 2007, this had shifted to:

> Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.[87]

And by 2009, this had shifted yet again to:

> Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings.[88]

Others have used infographics to make the dry contractual language come alive. Developer Matt McKeon, then at IBM Research and now at Google, created images depicting snapshots in time of Facebook's privacy policy, this one showing 2005:[89]

[84] Kevin Bankston, *Facebook's New Privacy Changes: The Good, the Bad, and the Ugly*, EFF DEEPLINKS BLOG (Dec. 12, 2009), http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly.

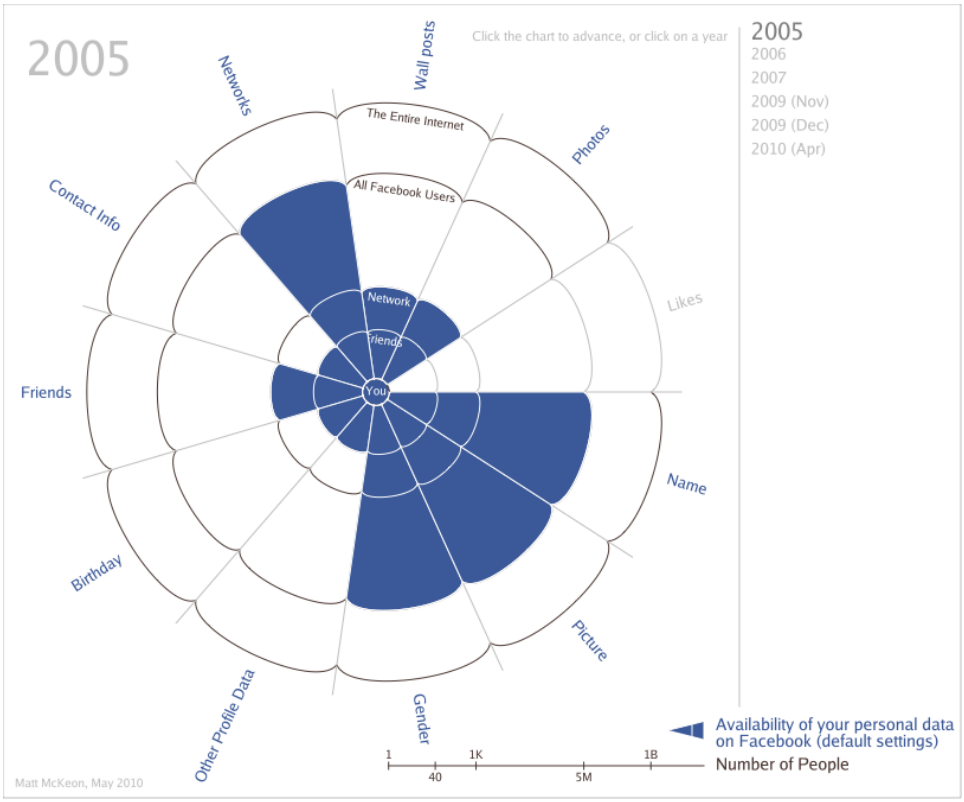
[85] Opsahl, *supra* note 78.

[86] *Id.*

[87] *Id.*

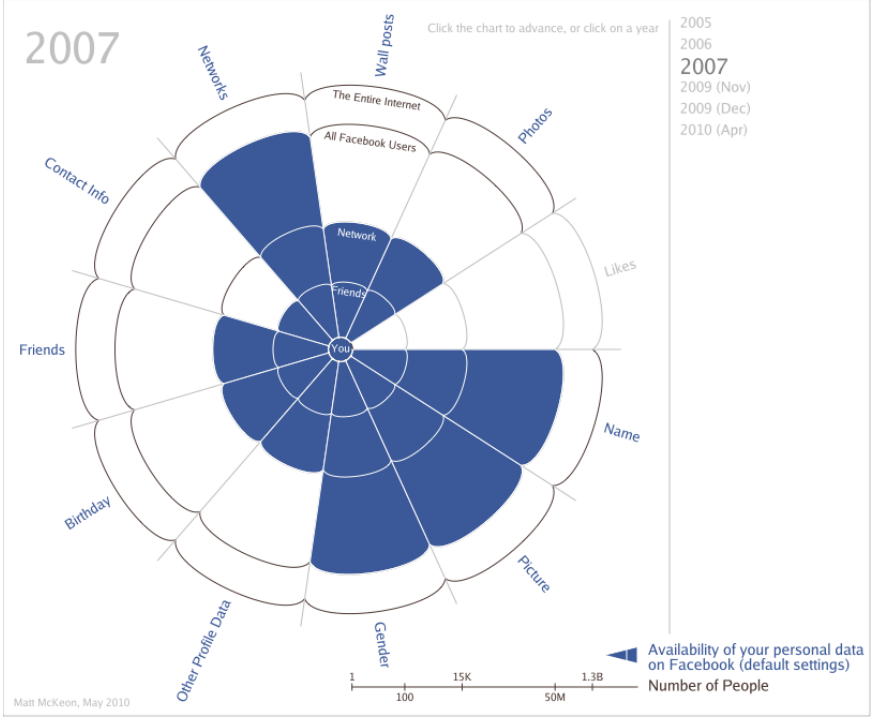
[88] *Id.*

[89] Matt McKeon, *The Evolution of Privacy on Facebook*, MATTMCKEON.COM, http://mattmckeon.com/facebook-privacy/ (last updated May 19, 2010).

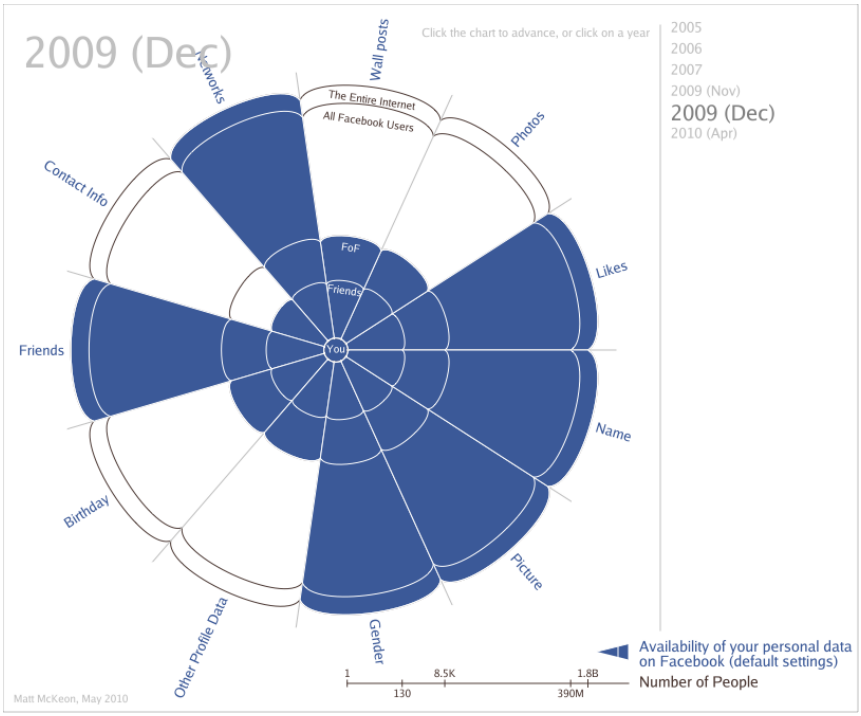



The image is a fine example of the visualization of law and policy and deserves close study. The growing concentric rings of the "flower" indicate larger populations of individuals, with the inner circle representing only "you" and the outer ring representing all users on the Internet. The graphic uses a logarithmic scale to indicate population, and the width of any ring represents the number of users. The "petals" of the flower indicate different categories of user-supplied information held by Facebook, all of which some might fairly classify as "sensitive" and some we might even consider "highly sensitive." The crossing of petals with rings produces individual cells shaded to indicate accessibility or left white to show inaccessibility. Thus, in 2005, all Facebook users could see a particular user's name, picture, gender, and networks, but nothing else, while "Friends" could see everything.

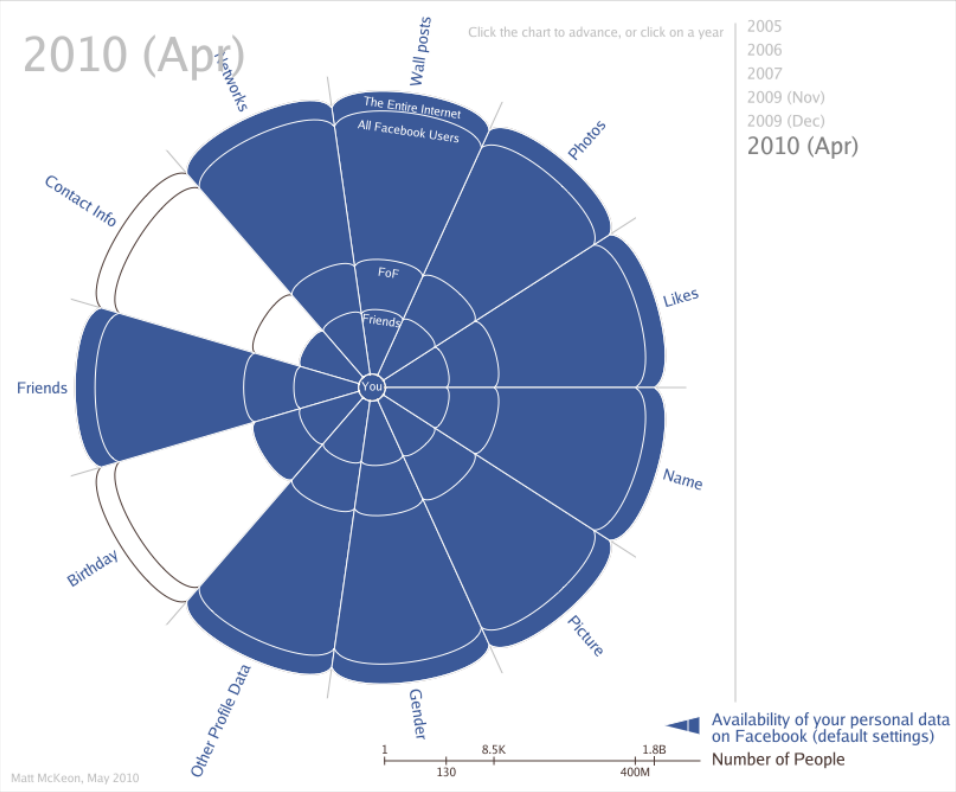
From 2005 to 2007, Facebook steadily increased what could be seen by default by others in a user's network, yet kept visibility beyond networks static and prohibited visibility from the rest of the Internet, resulting in the following picture:




By December 2009, Facebook knocked down the wall between itself and the Internet, and everybody (most importantly Google's spider) could then view a user's name, picture, gender, likes, and friends:



And in 2010, the transformation to a de facto public service was nearly complete, with only a user's birthday and contact info still relatively restricted and (importantly) with the user's "wall posts" revealed publicly by default for the first time.




Noticing Facebook's fundamental privacy lurch requires one to take a longer temporal view. At each step, Facebook exposed to public view a little more information from a user's profile page than it had before. Taken individually, these steps might seem like small shifts to the status quo, but when viewed across a still-relatively-compact set of five years, the radical sum shift is unmistakable.

As in the other three examples, Facebook's privacy lurch was criticized by consumers and privacy watchdogs and investigated by regulators. In 2011, the FTC filed charges against the company.[90] The two parties settled the charges late in 2011 with a consent settlement that binds Facebook to enhanced scrutiny of privacy practices for twenty years.[91]

It would be charitable for us to assume that Facebook's privacy lurch happened because of dynamic pressures from competitors rather than as a cynical ploy to bait-and-switch new users. But we should worry that it might instead be the latter and thus represent an intentional, emerging new business strategy: companies may use privacy lurches strategically to take advantage of the lock-in and even natural monopoly tendencies of services like

[90] In re Facebook, Inc., No. 092 3184, Complaint (F.T.C. Nov. 29, 2011).

[91] Fed. Trade Comm'n, Press Release: Facebook Settles FTC Charges That it Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm.

search engines and social networks.[92] The strategy works like this: create an online service with robust privacy practices, which will help lure people in. Once these people (now the service's users) have invested their time, energy, and social capital in the service and begin to feel the lock-in effects of networks and familiarity, the service pivots, shifting toward looser privacy policies that provide better profit-making opportunities. The users, with their privacy expectations dashed, will have no way to leave.

## C. The Problem with Privacy Lurches

Most privacy analysts weigh the impact of a privacy lurch by assessing only the information-handling practices that result from the lurch. In this way, analysts treat a lurch no differently from the way they treat a brand new practice. Thus, Facebook's decision to expose more information about its users to the general public should be assessed in precisely the same way we would assess a brand new social networking service that had made the same privacy choices. We miss something important if we treat a privacy lurch as no more than its end-state.

Privacy lurches give rise to two distinct sets of privacy harms, which I will call static and dynamic. The traditional approach to privacy analysis focuses solely on the static harms, those that stem from a company's new information-handling procedures. Consider the static harms resulting from two of the scenarios presented above: when Google knocked down the walls that had once separated databases, it created much more than a sum of the parts, revealing through the combination sensitive new bits of information that its users had consciously held back.[93] When Facebook exposed once-private information about its users to the general public and to Google's indexing spiders, it released embarrassing information (or worse) to stalkers, harassers, ex-spouses, potential employers, and more.

For the past decade, information-privacy theorists have been developing taxonomies and theories to describe privacy harms like these. None is as rich or complete as Dan Solove's taxonomy, which breaks privacy harm into four categories—information collection, processing, dissemination, and invasions—further subdivided into sixteen subcategories.[94] The static harms that result from a privacy lurch are no different than the harms that would have resulted had the company embraced the practices from the outset, which means that they may fall within every part of Solove's taxonomy. Google's decision to break down the walls between databases risks raising the harms of, at least, Solove's subcategories of surveillance, aggregation, identification, secondary use, exclusion, breach of confidentiality, disclosure, increased accessibility, and distortion.[95] Facebook's shift from private to public triggers the possibility of many of these same harms.

It is helpful to focus on the static harms resulting from a lurch, because they can be compared to the industry status quo. Facebook's shift from private to public can and should be compared to the practices of other social networking sites, such as Twitter, which has been public from birth.

---

[92] *See* Bracha & Pasquale, *supra* note 167.

[93] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (describing how for privacy, aggregated data is often more than the sum of its parts) [hereinafter Ohm, *Broken Promises*]; SOLOVE, THE DIGITAL PERSON, *supra* note 1 (same).

[94] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 101–06 (2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY].

[95] *Id.* at 104–05.

But this Article sheds light on the special problems of dynamism and change, problems that reflect not only the new data handling policies governing data about users, but harms that arise from the change itself. These are the harms felt by those who have their expectations of privacy dashed.[96] Sometimes, these people experience what might feel like new, independent harms. More often, a privacy lurch accentuates or magnifies the static harms they feel. These dynamic harms can be more disruptive and harmful than the static harms themselves.

Change can be deeply unsettling. Human beings prefer predictability and stability, and abrupt change upsets those desires. Dan Solove has noted these psychological effects, describing how the "secondary use" of information "generates fear and uncertainty" and "creat[es] a sense of powerlessness and vulnerability."[97] Helen Nissenbaum describes the "unexpected jolt" people experience when they are forced into a "clash of contexts."[98] We experience unexpected shifts as "nasty surprises of discovery."[99]

Rapid change causes harm by disrupting settled expectations. This exacerbates the psychological impact, causing feelings of "betrayal."[100] This betrayal may even extend beyond psychological and into an actual breach of contract if the change calls into question the validity of a binding promise between the user and the service.[101] When companies lurch, individual consumers can be made to feel as if they no longer have what they initially bought.[102] When instability becomes the norm, people may lose trust in the companies selling services or even entire industries.[103] Some lurches cause information to flow to friends or family in unintended ways, disrupting our most important social connections.[104]

Whether or not a privacy lurch constitutes contract breach, it treats people unfairly, disrupting the goals of consumer protection.[105] Privacy lurches can be unfair when they occur after a user has been coaxed into volunteer-

---

[96] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009) (describing breaches of norms of information flow).
[97] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 94, at 132.
[98] NISSENBAUM, *supra* note 96, at 205.
[99] *Id.*
[100] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 94, at 131.
[101] *E.g.* Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635 (2011).
[102] Grimmelmann, *Saving Facebook*, *supra* note 4, at 1169 ("If you—like most people—formed your privacy expectations around the way the site originally worked, they ceased being valid when the site changed.").
[103] U.S. Dep't of Commerce Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework at 1 (2010) (Privacy "harms . . . undermine consumer trust in the Internet environment [which] may cause consumers to hesitate before adopting new services and impede innovative and productive uses of new technologies . . . ."), available at http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.
[104] Grimmelmann, Saving Facebook, *supra* note 4, at 1169 (describing controversy after Friendster introduced the ability for users to see which other users had viewed their profiles); McGeveran, *supra* note 12 at 1123–24 (recounting how some users had surprise Christmas gifts ruined when Facebook Ads revealed purchases to their recipients).
[105] I am using "unfair" here in the non-legal, colloquial way. Later, the article will take up the more precise meaning in the FTC Act. *Infra* Part III.C.2.

ing personal information based on promises of privacy that no longer apply.[106] After a lurch, a service is no longer the thing the consumer thought he had agreed to buy; it is something much more harmful, possibly not worth the positive things the user enjoys in return. A privacy lurch can also unfairly decontextualize an individual, who might have produced different or additional information had he known the full extent to which his data was to be used.[107]

Within a liberal theory frame, abrupt change can work dignitary harms by "denying people control over the future use of their data, which can be used in ways that have significant effects on their lives."[108] Moreover, as privacy lurches proliferate, we might be left unwilling to trust the status quo, which might lead us to self-censorship and disrupt our ability to develop in ways we otherwise would.[109]

Even in Julie Cohen's post-modernist view of privacy, in which change itself is not a bad thing, abrupt change is problematic. "Vulnerability to environmental disruption" can sometimes inspire people to develop the "play of everyday practice" that she identifies as the central goal of good information policy.[110] When ground rules change, people "are quick to appropriate unexpected juxtapositions of spaces and resources . . . toward their own particular ends."[111] Privacy thus should be about creating enough "breathing room" for people to engage in "socially situated processes of boundary management."[112]

Still, Cohen is likely to criticize the kind of change described in this Article not because change itself is bad, but because the change operates only in one direction, toward increasing surveillance and away from privacy.[113] She finds privacy's value in the way it creates fixed boundaries between people and society to enable each individual to engage in "dynamic, emergent subjectivity from informational and spatial constraint."[114] "[P]rivacy must balance a type of fixity against a type of mobility . . . ."[115]

Ultimately, exposing users to an ever-shifting landscape of broken promises of privacy, in which every privacy policy is inconstant, whittles away expectations of privacy. I mean this in both the everyday and the legalistic meaning of the phrase. Expectations of privacy set our shared norms.[116]

---

[106] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 94, at 131 ("People might not give out data if they know about a secondary use, such as telemarketing, spam, or other forms of intrusive advertising.").

[107] *Id.* at 132 ("When data is removed from its original context in which it was collected, it can more readily be misunderstood."). ARTHUR MILLER, THE ASSAULT ON PRIVACY (1971) ("[An] individual who is asked to provide a simple item of information for what he believes to be a single purpose may omit explanatory details that become crucial when his file is surveyed for unrelated purposes.").

[108] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 94, at 131. Cohen, *supra* note 10, at 1423–24.

[109] Cohen, *supra* note 10, at 1423–24; ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959); ALAN WESTIN, PRIVACY AND FREEDOM 23–51 (1967).

[110] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE, 56 (2012).

[111] *Id.*

[112] *Id.* at 149.

[113] *See* Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1682 (1999) (describing "one-sided bargains that benefit data processors").

[114] COHEN, *supra* note 110, at 149.

[115] *Id.*

[116] *See* United States v. Jones, ___ U.S. ___, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular

Constant privacy lurches create a "widespread individual ignorance" about the way information is used which in turn "hinders development through the privacy marketplace of appropriate norms of individual use."[117] Scott McNealy's quote that "You have zero privacy. Get over it"[118] becomes self-fulfilling prophesy, as users are conditioned to assume that privacy is trending toward zero online. If we allow this kind of corporate-driven norm redefinition to go unchecked, users-qua-citizens could become a governing majority. We cannot create a system in which people live their lives without privacy and treat the ever-increasing number of people whose lives are destroyed by privacy harms as the victims of forces outside their control.[119]

More legalistically, diminishing expectations of privacy might feed into Constitutional law, because the Fourth Amendment is tied to the so-called "reasonable expectations of privacy" test.[120] Prosecutors have cited the low-level of privacy provided in online service privacy policies as a reason they can order the release of copies of electronic mail[121] or identify the location of cell phones[122] without probable cause or a warrant.[123] Arguments like these will strengthen and multiply over time, as company practices push users to expect privacy in fewer situations.[124]

## D. It Will Get Worse

The recent evolution of the market for online services leads us to the confident prediction that privacy lurches will happen more frequently across more industries in larger steps. Many companies are actively reshaping their business models to try to profit from customer secrets, and by doing this, they find themselves in a large, diverse market, squaring off against competitors from what used to be non-competitive market segments. Thus, cable companies compete not only against their historical competitors for broadband, the telephone companies, but also against websites and search engines, credit card companies, retailers (web-based and brick-and-mortar), streaming music websites, and e-book vendors.[125] In a unified market for consumer behavior, anybody who knows somebody else's secrets becomes a competitor.

In earlier writing, I labeled this the "Google envy" effect.[126] Google created an astronomical amount of value for its employees and shareholders by turning user searches into nickels, through the magic of contextual adver-

---

expectations are in flux and may ultimately produce significant changes in popular attitudes.").

[117] Schwartz, *supra* note 10, at 1683.

[118] A. Michael Froomkin, The Death of Privacy, 52 Stan. L. Rev. 1461, 1462 (2000).

[119] Jones, *supra* note 116 ("[E]ven if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

[120] U.S. CONST. AMEND. IV; Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring).

[121] Final Reply Brief for Defendant-Appellant United States, Warshak v. United States, 490 F.3d 455 (6th Cir. 2007) (No. 06–4092), vacated on reh'g en banc, 532 F.3d 521 (6th Cir. 2008), 2007 WL 2085416.

[122] Brief for the United States at 20–21, In re: Applications of the United States of America for Historical Cell-Site Data, No. 11-20884 (5th Cir. Feb. 15, 2012), available at http://epic.org/amicus/location/cell-phone-tracking/USA-Opening-Brief.pdf.

[123] Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012).

[124] *Id.*

[125] Ohm, *Rise and Fall*, *supra* note 51 at 1426.

[126] *Id.*

tising. Companies like Facebook, which soon will feel new shareholder pressure for profits, and broadband Internet providers are racing to do similar things in order to generate similar returns, they hope.[127]

These dynamic economic forces promise even more privacy lurches to come and spell disaster for privacy. Facebook and ISPs pour energy for innovation into thinking of ways to collect and monetize more information without angering their customers or government regulators. Google feels the pressure of competition nipping at its heels, and collects more information just to stay ahead.[128] Tens of thousands of other companies, including many companies that never before thought of themselves as involved in the sale or purchase of information, now try to mimic the Google model. The evidence of all of this energy becomes manifest in the large, and slowly increasing, size of databases collected by companies large and small. For the end user, the consumer whose data has become the object for trade in this market, the result is unsettling: a market in which promises and expectations of privacy lurch like the unsteady deck of a ship caught in turbulent waters.

## II. DEALING WITH PRIVACY LURCHES

We should find ways to protect users from the harmful, contract-breaching, dignity-impairing, psychologically jarring instability that occurs during privacy lurches. Based only on the broad literature of information privacy scholarship that has emerged during the past decade, we would first consider the two most commonly proposed types of solutions seemingly very different approaches at the opposite ends of a wide spectrum: aggressive regulatory intervention mandating the protection of substantive privacy rights on the one hand or transparent notice coupled with meaningful user choice on the other.[129]

But a surprise lurks. Once one focuses on privacy lurches alone, one realizes that these diametric opposites are not really very different after all. Any rights-based solution for the problem of privacy lurches, at least any that can muster enough political support to be enacted, does little more than devolve into notice and choice.

This is but the first example of a recurring theme: the large, unruly, messy law and policy landscape we encounter whenever we try to solve all of our information privacy problems simultaneously, simplifies dramatically when we narrow the lens to focus only on the problem of the privacy lurch. Solutions that seem like opposites are revealed to be variations on a single theme. Old problems and roadblocks disappear. New regulatory possibilities reveal themselves in places where none was seen before. This act of focus constitutes a clarifying and narrowing move, which I will call the focusing move, one which might make intractable problems in fact quite tractable.

If privacy lurch problems can be avoided only through notice-and-choice solutions, we still have a problem, because notice-and-choice solutions are deeply flawed. Notice and choice suffer from many well-recognized information quality problems that stem from the built-in limitations of a cluttered

---

[127] *Id.*

[128] Mat Honan, *The Case Against Google*, GIZMODO, March 22, 2012, http://gizmodo.com/5895010/the-case-against-google (describing dynamic economic forces pressuring Google to develop more privacy-invasive services).

[129] There is a third category, calls for the development of new technologies that make privacy problems go away. These solutions, such as they are, fall outside the scope of this Article.

online information environment and limits to human cognition. Too often, companies adopting a privacy lurch take advantage of these conditions to game notice and choice, in extreme cases they perform a bait-and-switch: join our privacy-protective service today and get stuck with a more privacy-invasive (and more profitable) new version tomorrow. We are left with a quandary. Only notice-and-choice solutions can protect us from the harms of privacy lurches, and all notice-and-solutions are flawed.

Once again, the focusing move provides a way around these flaws. Privacy lurches have special features that offer new ways around the problems with notice-and-choice.

## A. Traditional Approaches and their Shortcomings

### 1. Solving Smaller Privacy Problems

By focusing specifically on the privacy lurch, this Article embraces a growing trend in privacy scholarship, preferring solutions targeted for specific privacy problems over those that try to provide universal solutions. The most important example is Helen Nissenbaum's focus on what she calls "privacy in context" or "contextual integrity," and this Article echoes aspects of that work.

Many privacy scholars have given up trying to find a sweeping, universal approach to privacy. This move has been led by Daniel Solove and Helen Nissenbaum. Solove tackles privacy from a position of philosophical pragmatism.[130] He argues that "privacy issues should be worked out contextually rather than in the abstract" and faults theories that "are too general to provide much guidance for resolving concrete legal and policy issues."[131] Similarly, Nissenbaum focuses on what she calls "contextual integrity," a theory that requires us rigorously to account for how changes in technology affect what we have come to expect from the flow of information in a particular context to help explain how and when these expectations fail.[132]

A privacy lurch is not exactly a "context," at least as Nissenbaum uses the term. "Contexts are structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)."[133] Examples she discusses include voting, school, and social networks. A privacy lurch occurs across contexts like these.

But as Solove points out, we need to look beyond contexts alone. He tries to walk a tightrope between the specific and the general, arguing that "[v]iewing privacy more contextually alone often fails to provide sufficient direction for making policymaking or legal decisions, which depend upon generalizations."[134] Thus "we must navigate the tension between generality and particularity, between abstractness and concreteness."[135]

Nissenbaum also acknowledges that the focus on contexts must sometimes be supplemented by examinations of "cross-cutting concepts."[136] As one example, she asks us to pay "special attention [to] those challenges to the

[130] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 94, at 40.
[131] *Id.*
[132] Nissenbaum, *supra* note 96, at 128–29.
[133] *Id.* at 112.
[134] SOLOVE, UNDERSTANDING PRIVACY, *supra* note 94, at 48–49.
[135] *Id.* at 49.
[136] Nissenbaum, *supra* note 96, at 220.

status quo that involve a relaxation of constraints on information flow."[137] This sounds like she is talking about privacy lurches.

This Article attempts to walk Solove's tightrope by focusing on the privacy lurch as a useful compromise between more general and more contextual alternatives. By focusing only on lurches, we exclude the consideration of privacy problems involving brand-new business models (although these are discussed as a point of comparison throughout), government surveillance, and the ways users tend intentionally to share vast amounts of information about themselves with companies. This is not to suggest that those problems are less important or more difficult to solve, but instead recognizes the wisdom of drawing lines around tractable, important privacy problems without worrying unnecessarily about the cases that fall outside the line.

Solove and Nissenbaum define down privacy problems in order to force us to stop treating different things alike. But as I have argued, in this case, the focusing move does much more than that. By focusing on privacy lurches to the exclusion of other things, many persistent, vexing problems others have struggled to resolve surprisingly fade away. Focusing only on sudden, unexpected, and often unwanted change helps us simplify down much of the messy complexity of past privacy debates.[138]

### 2. Substantive Privacy Rights

In most privacy problems that have been assessed, the solutions tend to fall along a spectrum. At one end of the spectrum are solutions based on consumer notice and choice, the focus of most of the rest of this Article. At the other end of the spectrum are proposals that recognize privacy's special status as a fundamental human right.[139] These approaches suggest that privacy serves as a necessary precondition to human autonomy and development. Scholars writing in this vein spend time cataloging the ways in which privacy helps individuals and societies evolve and develop.[140] Without privacy, individuals do not enjoy liberty and cannot become fully-developed human beings. Given these stakes, rights-based accounts of privacy lead to prescriptions that are aggressive and burdensome to follow and favor universal over sectoral solutions.[141]

But when we make the focusing move, something surprising happens to this spectrum: it disappears. This is because the most aggressive rights-based approaches can never be enacted to attack privacy lurches. We cannot ban privacy lurches the way we might ban, for example, uses of extremely sensitive data. We are left instead with softer, squishier rules, most based on the so-called Fair Information Practice Principles (FIPPs). And a close examination of the relevant FIPPs demonstrate that these do little more than simple notice-and-choice, collapsing the spectrum into a single point.

---

[137] *Id.* at 221.

[138] To make a clumsy analogy to high school calculus, other theories of privacy tackle the privacy function, call it p(n), itself. This is a messy, wide-ranging, complex, and contextually diverse range of possibilities. This article in contrast looks only at the first derivative of the function, p′(n), considering only the rate of change in privacy, not the fixed value of privacy itself.

[139] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, art. 8, Nov. 4, 1950, ETS no. 005; Universal Declaration of Human Rights, United Nations General Assembly, art. 12, Dec. 10, 1948.

[140] Cohen, *supra* note 10; Schwartz, *supra* note 10.

[141] Kenneth Bamberger & Deirdre Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 256–57 (2011).

a) Ban Lurches?

The most straightforward—and easiest to dismiss—solution would be to ban privacy lurches outright. If instability is the source of the problem, then mandate stability. A new law could require that companies must declare at their birth their privacy commitments and then make it illegal to abandon any of those choices for the rest of the life of the company (or at least for a set number of years).

Because nobody has suggested a ban on lurches, the solution is merely a straw man, one that does not deserve much analysis. Let us quickly consider some of its shortcomings. First, such a rule would have a devastating effect on the dynamic marketplace for online services. Fixing companies into the pattern of behavior that they establish at the beginning and refusing to let them waiver from it sacrifices far too much for uneven gains to privacy.

Second, a blanket ban on lurches suffers from line-drawing problems. Surely we would not ban minor, insignificant, or immaterial shifts in privacy practices, so how should we draw the line? For these reasons, and others, a ban on lurches is not a viable solution.

b) Nissenbaum's Norms

A relatively new approach is one elaborated once again by Helen Nissenbaum, as part of her theory of contextual integrity. In a particular context, we should focus on whether people are breaching well-established norms of information flow.[142] Nissenbaum highlights two classes of norms in particular. Norms of appropriateness describe the uses of information that are fitting or traditionally expected or welcome in a given situation.[143] Norms of distribution tell us whether the flow of information to others complies with traditional expectations of confidentiality.[144]

What are the norms of appropriateness and distribution when a company decides to lurch? One naïve approach would be nearly tautological: a company's pre-lurch practices set the norms of distribution and appropriateness. Any material deviation from those practices thus constitutes a breach and should thus be considered a privacy concern, one we might regulate to avoid.

A more sophisticated account might try harder to elaborate the norms of change in a given context. Since the birth of the commercial Internet, companies have changed their privacy policies, and by this point there are probably well-established, if difficult to list, norms of change. The problem is that most of these norms allow for lurches in cases so long as consumers receive meaningful notice-and-choice. The difference between rights-based and notice-and-choice solutions proves illusory.[145]

c) FIPPs

Most of those who start by treating privacy as a fundamental human right end with some listing of Fair Information Practice Principles (FIPPs), which are lists of best practices for protecting information privacy promulgated by various organizations.[146] Many of the FIPPs, however, simply do not

[142] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).
[143] *Id.* at 138–40.
[144] *Id.* at 140–43.
[145] There are other norms that might depart from simple notice-and-choice. These are discussed further in Part III.
[146] Gellman, *supra* note 148.

apply to the problem of a privacy lurch. For example, many lists of the FIPPs require giving data subjects the right to learn all information held by a data processor and the separate right to demand the correction of mistakes.[147] These FIPPs are not directly applicable to the problems that arise during a lurch.

On the other hand, every list includes some FIPPs that target privacy lurches directly. For example, most lists include principles of "purpose specification" and "use limitation"[148] and refer to breaches of these particular practices as impermissible "secondary use."[149] The EU Data Protection Directive prohibits secondary use without consent.[150] Similar provisions are found in U.S. articulations of the FIPPs.[151]

Notice, however, that the various rules designed to operationalize these particular FIPPs do little more than require notice and choice, albeit often of a heightened form. Privacy lurches thus collapse the supposedly great divide between rights-based and market-based approaches into a unified focus on notice-and-choice. It is thus to notice-and-choice solutions that we now turn, and it is an improvement on traditional notice and choice that the rest of this Article develops.

### 3. Traditional Notice-and-Choice

#### a) General Principles

Notice-and-choice solutions enable market forces to provide consumers with the amount of privacy that their preferences—revealed and express—suggest they truly desire, even when they claim to want more. The bedrock of these solutions is the requirement that every consumer must be shown a detailed description of how information about him or her is collected, used, and shared.

When regulators embrace notice and choice, they tend to relegate their responsibilities to monitoring the data-handling promises being made by companies, ensuring that users are being presented detailed descriptions of those promises, usually in the form of a detailed privacy policy, and trying to detect circumstances in which promises are broken for further investigation or action. For most of the past decade, this describes the form of regula-

---

147 *E.g.* Directive 95/46/EC, *supra* note 150.

148 Robert Gellman, *Fair Information Practices: A Basic History,* BOBGELLMAN.COM (Feb. 23, 2012) http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

149 *Fair Information Practice Principles*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited March 19, 2012).

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

151 *E.g.* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf [hereinafter FTC PRIVACY REPORT] (explaining that a company that decides to treat "consumer data in a materially different matter," must first "provide prominent disclosures and obtain opt-in consent" or risk FTC action for unfair and deceptive trade practices); THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter WHITE HOUSE WHITE PAPER] ("If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice.").

tion that has been embraced by the FTC, which has identified notice as "[t]he most fundamental principle."[152]

Even outside the United States, notice and choice play a disproportionately important regulatory role. In the European Union data protection directive, for example, two paramount FIPPs are "Purpose Specification" and "Use Limitation," which operate not unlike the way the FTC implements notice and choice.[153]

Ryan Calo explains why notice-and-choice-based privacy regulations are popular with many parties.[154] Regulators view them as "cheap to implement and easy to enforce."[155] They see them as unlikely to significantly impair innovation.[156] Company representatives see notice-and-choice mandates as far less objectionable than the alternatives.[157]

b) Information-Quality Problems

Despite the popularity and widespread adoption of notice-and-choice rules for privacy, critics attack them unsparingly. Most of these critics focus on a broad list of what I label "information quality" problems.[158] Nobody reads privacy policies, and even if they did, they would not be likely to understand them, because they are often very long and full of legalese.[159] There are also too many privacy policies, especially as so much economic and social activity moves to the web.[160] Researchers at Carnegie Mellon estimated that it would cost the American economy hundreds of billions of dollars in lost worker productivity if every worker decided to skim every privacy policy encountered.[161]

Even worse, humans suffer from bounded rationality and cognitive biases that conspire to make us likely to misunderstand privacy policies.[162] Several surveys have found that many survey respondents believed that by publishing a document called a "privacy policy," a company promised to protect privacy, regardless of the content of the policy.[163] Others have suggested in studies that the ways privacy risks are framed have a significant effect on acceptance, with the best strategy (from the point of view of the company) to state things in vague or uncertain ways.[164] Consumers tend to

---

[152] *Fair Information Practice Principles*, *supra* note 149.
[153] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).
[154] Calo, *supra* note 11, at 121–23.
[155] *Id.* at 121.
[156] *Id.* at 122.
[157] *Id.* at 123 ("Mandated notice can and does face opposition, but opposition tends to be less fierce than to top-down dictates regarding what a company can and cannot do.").
[158] *See supra* notes 10–11.
[159] Bianca Bosker, *Facebook Privacy Policy Explained: It's Longer Than The Constitution*, HUFFINGTON POST (July 12, 2010), http://www.huffingtonpost.com/2010/05/12/facebook-privacy-policy-s_n_574389.html.
[160] *See* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. OF PA. L. REV. 647 (describing the "overload effect" in many contexts including online disclosure).
[161] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & POL'Y FOR. INFO. SOC'Y 543, 544, 564 (2008).
[162] Calo, *supra* note 11, at 125–28.
[163] Turow et al., *The FTC and Consumer Privacy in the Coming Decade*.
[164] Acquisti, *supra* note 11, at § 3.2.

trust the privacy practices of websites with a neat appearance and design, an example of the representativeness heuristic.[165] Other examples include the ways prospect theory, the endowment effect, and hyperbolic discounting have explained, in part, how people mis-assess privacy risk.[166]

c) Traditional Notice and Choice During a Lurch

It is critical to note how the problems with notice and choice seem greatly exacerbated during a privacy lurch. When a user signs onto a new service for the first time, she at least receives cues from the unfamiliarity of the service that trigger heightened attention to promises being made about information handling, if just a little. But after a user has settled into a service, she has little reason to continue to read changes to privacy policies.[167]

Consider the mechanics of notice and choice both during the initial launch of a company and after a privacy lurch. At the launch of a new service, several contextual clues mitigate some of the information-quality problems, yet these clues are absent during a lurch. For example, notice and choice during initial launch tends to follow a nearly invariant pattern: user presses the "sign up" button; user provides some basic registration information; user is presented with the terms of service and privacy policy; user must click "I Agree" to continue. This ceremony is the product of a combination of technical constraints, evolved user expectations, legal and regulatory pressures, and chance. Even though most users do not read the terms of service,[168] and even though we should not want most users to do so,[169] the highly evolved ceremony of notice and choice during initial launch gives users and their advocates a chance to notice the new service.

In contrast to this pervasive similarity, every lurch is different. Without the ceremony of initial login, each company approaches notice and choice around change in different ways, and many companies treat their own different changes at different times in different ways. Some companies—probably the minority—prevent users from engaging with the service until they see the terms of service and click "I agree" once again. Most companies allow the user to engage the service without interruption, but send notices and alerts about the change. Google, for example, pervaded its pages with small, highlighted notices throughout February 2012, all of which included the pithy catch-

---

[165] *Id.*

[166] *Id.* §§ 3.2, 3.3.

[167] There are also problems with choice, separate from the notice problems discussed in the text. Many online services are offered without any significant competition, meaning users are forced into take-it-or-leave-it situations. Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008).

[168] *See* Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J. OF L. & POL'Y 723 (2007) (reporting results of suvey finding that "only 1.4% reported reading EULAs often and thoroughly, 66.2% admit to rarely reading or browsing the contents of EULAs, and 7.7% indicated that they have not noticed these agreements in the past or have never read them"); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts*, NYU Center for Law, Economics and Organization Research Paper Series Working Paper No. 09-40 at 1 (October 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443256 (reporting that "only one or two out of every thousand retail software shoppers chooses to access the end user license agreement").

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

phrase, "This Stuff Matters." Some companies send out-of-band notices on blogs[170] or anachronistically on paper letters sent via snail mail.[171]

The problem, perhaps ironically, is communicative richness. Outside the ceremony of initial login, companies face a diverse and rich number of ways to communicate notice and to receive choice. Each company uses a rich canvas on which it can manipulate, decontextualize, and mislead, making every privacy lurch, no matter how invasive, seem like a boon to consumers. Even when companies change practices in ways that significantly reduce user privacy, they will often downplay the risk to privacy sometimes shifting the focus to the specious benefits to the users of the change. Notice and choice during a lurch is too often the name we give to corporate propaganda.

This communicative richness has given rise to a new form of corporate writing that one might almost appreciate for its craftiness and subtlety, if the results were not deception and harm: privacy lurch doublespeak.[172] For example, Google touted the benefits of its decision to tear down the walls between its databases as part of "efforts to integrate our different products more closely so that we can create a beautifully simple, intuitive user experience across Google."[173] When Charter Communications decided to begin monitoring its users in partnership with NebuAd, its letter to consumers touted the improved ads each customer would soon see: "[T]he advertising you typically see online will better reflect the interests you express through your web-surfing activity. You will not see more ads—just ads that are more relevant to you."[174] And Mark Zuckerberg's December 2009 blog post highlighted some privacy-friendly changes the company had made without hinting at the very anti-privacy changes made simultaneously.[175]

## B. Improving Notice and Choice During a Lurch

Traditional notice-and-choice approaches are thus not nearly enough to address the special problem of a privacy lurch. The FTC has acknowledged this, calling for special rules during times of "material" privacy change.[176] Others have seized on this problem, albeit not in the context of lurches alone, and have proposed different ways to improve notice and choice. The two most promising approaches have been to search for better forms of notice and

---

[170] Whitten, *supra* note 37; Mark Zuckerburg, *An Open Letter from Facebook Founder Mark Zuckerberg*, THE FACEBOOK BLOG, Dec. 1, 2009, 6:23 P.M., http://blog.facebook.com/blog.php?post=190423927130 (describing changes made to privacy policies).

[171] Charter Letter to Consumers, N.Y. TIMES, http://graphics8.nytimes.com/packages/pdf/technology/20080514_charter_letter.pdf (last visited Mar. 27, 2012).

[172] GEORGE ORWELL, 1984 (1949).

[173] Whitten, *supra* note 37.

[174] Charter Letter, *supra* note 171; Saul Hansell, *Charter Will Monitor Customers' Web Surfing to Target Ads*, N.Y. TIMES (May 14, 2008, 8:40 AM), http://bits.blogs.nytimes.com/2008/05/14/charter-will-monitor-customers-web-surfing-to-target-ads/.

[175] Zuckerberg, *supra* note 170. *See* Kevin Bankston, *Facebook's Privacy Changes: The Good, the Bad, and the Ugly*, EFF DEEPLINKS BLOG, Dec. 9, 2009, https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly.

[176] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 57–58 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC FINAL REPORT].

choice and to advocate a switch from opt-out to opt-in adoption of new features. Neither one does enough to take on the significant information-quality problems during a privacy lurch.

1. Better Forms of Notice

Many researchers have proposed ways to improve on text-heavy privacy policies. Most of these proposals have turned to tables and symbols to try distill dozens of choices into more user-friendly formats. Researchers have long talked about finding a "nutrition label" equivalent for privacy policies.[177] Lorrie Cranor's research group at Carnegie Mellon is a leader in this field, and has proposed several alternatives, heavy with symbols and grids.[178] FTC consultants have proposed standardized privacy notices for the financial industry.[179] Many others have proposed different alternatives.[180]

But although each of these alternative designs is an improvement on text-based privacy policies, none seems to do a much better job than a privacy policy of being noticed and understood.[181] None of the simplified labels seems simple enough. Studies have shown that many of them continue to confuse people.[182] None has been widely embraced, despite endorsements from important regulators.[183] The authors of the new designs themselves acknowledge continuing shortcomings and continue to search for something better.[184]

What has sunk every one of these efforts is the inherent complexity of the problem. These researchers have all started from the proposition that companies should be able to use information in any way they see fit, and accordingly, privacy notices must be plastic enough to accurately represent every possible permutation of information-handling practices.

The pressure toward complexity comes not only from a desire to give companies the freedom to use information in every possible permutation; it comes from the other direction as well, from privacy watchdogs searching for tools that will lead to consumers making informed choices. Given the highly

---

[177] Patrick Gage Kelley, A "Nutrition Label" for Privacy, 2009 Symp. on Usable Privacy and Security; Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1 (2009).

[178] Reeder, R., Cranor, L., Kelley, P., and McDonald, A. A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization. Workshop on Privacy in the Electronic Society.

[179] Kleimann Communication Group, Inc. Evolution of a Prototype Financial Privacy Notice. February 2006.

[180] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254 (2010) (testing efficacy of privacy icons); Alan Levy & Manoj Hastak, Consumer Comprehension of Financial Privacy Notices (Dec. 15, 2008) (report prepared for seven federal agencies suggesting the use of tables in financial privacy disclosure); The Center for Information Policy Leadership, Hunton & Williams, *Multi-layered notices*.

[181] Calo, *supra* note 11, at 107 ("Studies show only marginal improvement in consumer understanding where privacy policies get expressed as tables, icons, or labels, assuming the consumer even reads them.").

[182] Alan Levy & Manoj Hastak, *Consumer Comprehension of Financial Privacy Notices* (Dec. 15, 2008); Patrick Gage Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, CMU-CyLab-90-014 (Jan. 12, 2010).

[183] FTC FINAL REPORT, *supra* note 176, at 62.

[184] Aleecia M. McDonald et al., *A Comparative Study of Online Privacy Policies and Formats*, PROCEEDINGS OF THE 9TH INTERNATIONAL SYMPOSIUM ON PRIVACY ENHANCING TECHNOLOGIES (Ian Goldberg & Mikhail J. Atallah eds., 2009).

contextual nature of privacy preferences,[185] the more details we can provide consumers, the better informed they will be.

These pressures that drive toward complexity seem always to outweigh countervailing desires for simple and easy-to-digest designs. Every one of the new designs summarized above contains dozens of words and a blur of icons, colors, and grids.

Privacy, in other words, is not nutrition, according to the top minds who have considered the disclosure problem. With a nutrition label, most people are interested most in calories, which is thus given a place of prominence on the top line. Those with more individualized needs—for example, those seeking a particular mineral supplement or engaged in a low-carbohydrate fad diet—will find some of the information they want further down the label. But despite catering to many needs, a nutrition label contains a mere fraction of the amount of information contained in any of the "simplified" privacy labels presented above.

Focusing on the privacy lurch offers a way out of the complexity quagmire. In order to assess a lurch, we do not need to consider the entire infinitely rich set of ways companies can collect, use, and share information. Instead, we can ask a simpler, more isolated question: how much has this company departed from its original privacy commitments? In some cases, the answer to this question will be gloriously reducible to a single quantity: this company has doubled the number of people who can touch the information, or it has tripled the amount of time it retains the data. There of course will continue to be significant variability in the way we measure and talk about privacy change, but the problem seems fundamentally simpler than the "anything and everything" problem tackled by the researchers described above.

And the simplicity of describing the impact of a privacy lurch leads directly to new, better forms of notice that are much more compact and much easier to understand. One might imagine a "green/yellow/red" light system summarizing how much a company has shifted away from its key privacy commitments.[186]

### 2. Opt-In Versus Opt-Out

Those who have focused on the special problem of the privacy lurch before have almost always focused on the opt-in/opt-out distinction. The FTC has declared that when companies make changes to "material" privacy policies, users should not need to live under them unless and until they opt in to the change.[187] Companies would much rather automatically migrate all of their users over, giving users the chance to opt out of the change, perhaps coupled with mandatory notice requirements.

People have placed too much emphasis on the difference between opt-in and opt-out. Requiring opt-in is not sufficient to address the privacy problems of a privacy lurch due to the information-quality problems discussed above. In fact, these information-quality problems are made worse during a lurch. Consider again the problem of Orwellian doublespeak, as in the Google and Charter examples, problems that are abetted by the modes and media of information delivery used today to deliver notice of a lurch. The mere act of

[185] *See* NISSENBAUM, *supra* note 96, at 109.

[186] Much will turn, of course, on how we identify the "key" commitments, a question taken up in Part III.B.1.

[187] FTC FINAL REPORT, *supra* note 176, at 57–58.

giving users the opportunity to voluntarily enroll in a new service is not enough if companies are permitted to trick them into making the choice.

Another reason opt-in is not sufficient is because people often do not have a meaningful alternative to choose from. [more]

But if we could find a way to improve the information-quality problems that plague today's privacy lurches, then meaningful opt-in could serve as a bulwark of privacy in the face of change. Privacy lurches are extremely disruptive events with the potential to confound expectations and lead to unwanted privacy harm. The FTC and others are correct to argue that many lurches require opt-in.

It might be, however, that curing the information-quality problems alone is sometimes enough, meaning that opt-in is not necessary, as well as not sufficient, for protecting privacy during a lurch. If we could somehow identify an improved form of notice that clearly and unambiguously signals to the consumer that an important privacy commitment has changed, the notice itself might signal to end users and privacy watchdogs alike the importance of the change. In some cases, the resulting publicity, debate, and regulatory scrutiny might itself cause people to focus more on whether and how to opt out, closing the gap between opt-in and opt-out, and serving as an improvement on today's world of bad information and opt-in.

#### 3. Summarizing the Critique

Prior attempts to protect privacy during a lurch run headlong into two significant problems: instability and information quality. The expectation-defying instability of a lurch gives rise to the harms discussed in Part I. The information-quality difficulties of the online environment explain why traditional notice-and-choice approaches do not do enough to protect privacy. Of greatest concern is the way the communicative richness of notice and choice during a lurch has given companies the means to engage in privacy lurch doublespeak. Luckily, there is an entire area of information-policy doctrine and theory—the study of trademarks and brands—that provides tools for both protecting consumer expectations from charges of instability and for improving information quality.

## C. Leveraging Trademarks

Critics of notice and choice decry the fundamental information-quality problems associated with online privacy policies.[188] Given how often complaints like these have been made, it is surprising that nobody has previously considered trademarks and brands, which serve as perhaps the most powerful symbols in the consumer marketplace, for novel solutions.[189] Trademarks can provide precisely what is needed to remedy the instability and information-quality problems at the heart of the problems with privacy lurches.

#### 1. Trademarks,[190] Brands and the Law

The law has recognized the commercial importance of marking goods and services since antiquity. From the first time a potter placed his distinctive mark on his wares, merchants have used words and symbols as infor-

[188] *Supra* Part I.A.1.

[189] *Supra* note 12.

[190] For most of the online services discussed in this Article, the relevant marks are service marks not trademarks. *See* 15 U.S.C. § 1127 (defining "trademark" and "service mark"). But to simplify the discussion, this Article will use the word "trademark" throughout.

mation devices, efficient means to communicate to potential customers that the product or service has been backed by a known source who guarantees a specific level of quality and accountability.[191] Today, governments provide legal support to bolster and protect the information function of these words and symbols, through trademark and other unfair competition laws.[192]

Trademark law extends protection to the first user of a distinctive mark in commerce.[193] For marks that are words (as opposed to symbols such as logos) distinctiveness is measured along a scale from generic to descriptive to "inherently distinctive," a category further subdivided into suggestive, arbitrary, and fanciful.[194] Inherently distinctive marks are protected upon first use,[195] but descriptive marks cannot be protected until the consuming public associates "secondary meaning" with them, which is often demonstrated through the use of surveys.[196] The Lanham Act, the federal trademark law, implements a national registration system, through which trademark owners can register marks giving them a range of procedural advantages at trial and putting competitors on constructive nationwide notice.[197] A civil complaint for trademark infringement is an allegation by a user of a mark that another is using a mark in a confusingly similar way.[198] Prevailing parties are entitled to damages, fees, injunctions, and the destruction of infringing articles.[199]

Trademarks implicate laws beyond trademark law, when they are treated as communications from producers to consumers.[200] By using a particular trademark, a producer makes claims about the qualities of his good or service. If these claims turn out to be false, laws that prohibit commercial deception, and most importantly false advertising law, might be triggered.[201]

2. The Information Quality Power of a Name

This Article does not argue that traditional trademark law and theory says much about the problem of the privacy lurch. In fact, traditional theory treats trademarks as nothing more than symbols of source alone.[202] During a

---

[191] FRANK I. SCHECTHER, THE HISTORICAL FOUNDATIONS OF THE LAW RELATING TO TRADE-MARKS (1925).

[192] William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 J.L. & ECON 265 (1987)

[193] 15 U.S.C. § 1125(a).

[194] Abercrombie & Fitch Co. vs. Hunting World, Inc., 461 F.2d 1040 (2d Cir. 1972).

[195] *But see* 15 U.S.C. § 1051 (permitting registration of a trademark before use if registrant has bona fide intent to use).

[196] Park 'N Fly, Inc. v. Dollar Park & Fly, Inc., 469 U.S. 189 (1985).

[197] 15 U.S.C. §§ 1051–72.

[198] 15 U.S.C. §§ 1114, 1125; Polaroid Corp. v. Polarad Elecs. Corp., 287 F.2d 492 (2d Cir. 1961).

[199] 15 U.S.C. §§ 1116–18.

[200] J. Shahar Dillbary, *Getting the Word Out: The Informational Function of Trademarks*, 41 ARIZ. ST. L.J. 991 (2009).

[201] *E.g.* Abbott Labs v. Mead Johnson & Co., 971 F.2d 6, 14 (1992) (finding use of mark "Ricelyte" to be false advertising under Lanham Act § 43(a)(1)(B) because the product contained no rice ingredients).

[202] Stacey L. Dogan & Mark A. Lemley, *Trademarks and Consumer Search Costs on the Internet*, 41 HOUS. L. REV. 777, 788-89 (2003) ("Trademark law thus historically limited itself to preventing uses of marks that 'defrauded the public' by confusing people into believing that an infringer's goods were produced or sponsored by the trademark holder."); Smith v. Chanel, Inc., 402 F.2d 562, 566 (9th Cir. 1968) ("[T]he only legally relevant function of a trademark is to impart information as to the source or sponsorship of the product.").

privacy lurch, consumers are often misled about the nature and quality of the service they are using, but they are rarely confused about the identity of the company providing the service.[203]

We will return to trademark theory in Part III, but for now, I am making a descriptive claim about the words and symbols we call trademarks themselves rather than a broader claim about the theory of trademark law. Trademarks are considered worthy of legal protection because consumers tend to associate them with meaning, and this happens because trademarks are designed to be efficient delivery mechanisms for meaning. To put it another way, trademarks are well-engineered meaning machines. Although scholars and courts have often noted the way trademarks take on meaning, they rarely explain why these particular words and symbols, and not others, serve this function so well.[204] But to support the claim that a trademark can do a better job communicating with consumers during a privacy lurch than traditional forms of notice-and-choice, we need to lift the hood on the meaning machine. Trademarks impart meaning for reasons that can be divided into three categories: the inherent qualities of trademarks, the engineered attributes of trademarks, and the way trademarks tend to be used.

First, trademarks act like meaning machines because of their inherent qualities, which in turn flow from the way the law defines a protectable trademark. Trademarks in any form—text, logos, slogans[205]—tend to be simple and short. Most textual trademarks range from single words to short slogans, and "the longer the slogan, the less probability that it functions as a trademark."[206] Designs and symbols can also serve as trademarks, but again, most trademarks tend to be simple, not ornate.[207]

Because trademarks convey meaning in an efficient and compact form, they are much easier for a consumer to understand than a typical privacy policy, dozens of pages, full of dense, incomprehensible legalese. Consumers can easily allocate the time and attention to "read" a trademark, and almost no consumer will fail to notice when a trademark changes.

The brevity of a trademark can counter the doublespeak problem too often encountered during a privacy lurch.[208] By letting companies announce privacy promises using screens full of text alone, we invite evasion and confusion. If instead we could use the trademark as a principal channel for communication to the consumer about important privacy changes, we could constrain the harmful creativity of privacy counsel.

The other inherent reason trademarks impart meaning is perhaps the most elemental: a trademark is a name. Trademarks are intertwined in complicated ways with a company's identity.[209] Consumers collect impressions about their interactions with a company over time, and they build those impressions into a mental model linked directly to the name. The name itself creates a mental placeholder for those impressions.

---

[203] *Infra* Part III.A.2.

[204] Mark A. Lemley, *The Modern Lanham Act and the Death of Common Sense*, 108 YALE L.J. 1687 (1999) ("Trademarks are a compact and efficient means of communicating information to consumers.").

[205] 15 U.S.C. § 1127.

[206] J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 7:20 (4th ed. 2007).

[207] *Id.* at § 7:24.

[208] *Supra* notes 172-175 and text accompanying.

[209] Laura Heymann, *Naming, Identity, and Trademark Law*, 86 IND. L.J. 381 (2011).

Second, trademarks are meaning machines because they are engineered to be so. Companies do not select trademarks on a whim; instead, they employ experts in marketing and advertising to engineer marks that exploit human psyche and cognition, burning particular meanings into memory. For decades, researchers have explored the cognitive and psychological mechanisms that give trademarks their power to conjure positive brand associations. Marketing experts have developed strategies for building better, more memorable and meaningful trademarks, manipulating word structure,[210] component meaning,[211] sound,[212] color,[213] typeface,[214] and imagery.[215]

Marketing professionals use these tactics and others to create brand symbols that are imbued deeply with meaning.[216] The law does not grant trademark rights to arbitrary symbols. It is only when symbols are associated in the mind of the consumer with particular meaning that the law applies.

The third set of reasons trademarks act as meaning machines and thus address some of the shortcomings of privacy notice-and-choice stems from the way trademarks are used by producers. Producers almost always display trademarks prominently. In fact, a buried symbol will probably not even earn protection.[217] Often, a product's trademark will be the largest element on its label.[218] On the web, the principal service mark is almost always posted directly at the top of the page, well above the virtual "fold" demarcated by the bottom of the browser screen.[219] Almost always, the logo or name is placed in the upper left or middle left of the web page, areas research indicates are the first a consumer views.[220]

Not only do producers display trademarks prominently, but also they use them consistently. At least with established brands, producers often change a name or logo only after great deliberation and study. In fact, the launch of a redesigned logo is often a time of internal anxiety and external attention, as companies build marketing campaigns to tout new logos and the

---

[210] Ira Schloss, *Chickens and Pickles, Choosing a Brand Name*, 21 J. ADVERTISING RESEARCH 47 (1981).

[211] Kevin Lane Keller et al., *The Effects of Brand Name Suggestiveness on Advertising Recall*, 62 J. MARKETING 48 (1998).

[212] Richard R. Klink, *Creating Brand Names with Meaning: The Use of Sound Symbolism*, 11 MARKETING LETTERS 5 (2000).

[213] *Id.*

[214] Terry L. Childers & Jeffrey Jass, *All Dressed up with Something to Say: Effects of Typeface Semantic Associations on Brand Perceptions and Consumer Memory*, 12 J. CONSUMER PSYCHOLOGY 93 (2002).

[215] Rebecca Tushnet, *Looking at the Lanham Act: Images in Trademark and Advertising Law*, 48 HOUS. L. REV. 861 (2012).

[216] Beebe, *supra* note 13.

[217] Ex parte Procter & Gamble Co., 96 U.S.P.Q. 272 (Chief Examiner 1953) (noting that trademark law "clearly does not contemplate that the public will be required or expected to browse through a group of words or scan an entire page to decide that a particular word or words are intended to identify the product of applicant").

[218] *See* MCCARTHY, *supra* note 206, at § 7:3 ("[T]he prominence of a word or symbol is certainly an important element in determining whether it creates a separate commercial impression on the average buyer.").

[219] *See* Shaun Cronin, *Designing for the New Fold: Web Design Post Monitorism*, WEBDESIGN TUTS+, Jan. 25, 2011, http://webdesign.tutsplus.com/articles/design-theory/designing-for-the-new-fold-web-design-post-monitorism/.

[220] Jakob Nielsen, *F-Shaped Pattern for Reading Web Content*, http://www.useit.com/alertbox/reading_pattern.html.

way they reflect their corporate values and qualities, while the web's chattering classes debate each redesign.[221]

3. Trademarks as Symbols of Privacy Practices

Orthodox trademark law tends to focus on only one particular type of meaning, the identity of the source of the product or service.[222] But because trademarks are meaning machines, they tend to become associated by consumers with many other meanings in addition to source, including attitudes about a company's approach to privacy. Before turning, in the next Part, from the descriptive to the prescriptive, consider one more way privacy and branding tend already to be intertwined.

Companies understand how naming can increase the visibility of a privacy lurch. In 2010, Google launched Google Buzz, a platform for social networking layered atop Gmail,[223] but the company ill-advisedly decided to automatically enroll all Gmail users and even revealed publicly each user's most frequent Gmail correspondents.[224] In 2007, Facebook launched Facebook Ads and Facebook Beacon, together a "social marketing" advertising platform that caused users to become the unwitting social spokespeople for companies whose products they bought.[225] Both launches ended disastrously, as consumers first and then regulators next became concerned about the implications for privacy.[226] In both cases, the FTC initiated actions against the companies, which resulted in sweeping consent agreements.[227]

Contrast Facebook Beacon with Facebook's slow migration from private to public, and Google Buzz to Google's decision to tear down the walls between its databases. In privacy circles, Buzz and Beacon are widely seen as disasters, deplorable decisions that justifiably attracted regulatory scrutiny and ultimately were driven out of existence. The other two decisions, while criticized, have not yet drawn the same kind of intense criticism, although it is still a bit too early to tell in the case of Google's database decision.

These side-by-side comparisons demonstrate the power of a name. We should not be surprised that branded shifts have generated more negative meaning in the minds of consumers than unbranded shifts made by the very same companies. A name casts a spotlight on an event in ways that focus the

---

[221] One blog describes its mission this way: "[Our] sole purpose is to chronicle and provide opinions on corporate and brand identity work, focusing mostly on identity design and a modest amount of packaging. We cover redesigns and new designs. Nothing more, nothing less, what you see is what you get." About Brand New, http://www.underconsideration.com/brandnew/about-brand-new.php (last visited July 13, 2012).

[222] *Supra* note 202.

[223] Edward Ho, *Google Buzz in Gmail*, OFFICIAL GOOGLE BLOG (Feb 9, 2010, 11:00 EST).

[224] Molly Wood, *Google Buzz: Privacy Nightmare*, CNET (Feb. 10, 2010), http://news.cnet.com/8301-31322_3-10451428-256.html.

[225] Louise Story, *Facebook Is Marketing Your Brand Preferences (with Your Permission)*, N.Y. TIMES, Nov. 7, 2007, at C5.

[226] Nicholas Carlson, *WARNING: Google Buzz Has a Huge Privacy Flaw*, BUS. INSIDER: SILICON ALLEY INSIDER (Feb. 10, 2010), http:// www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2; Steven Levy, Do Real Friends Share Ads?, Newsweek, Dec. 10, 2007, at 30 (noting that more than 30,000 Facebook users joined the Facebook group "Facebook: Stop Invading my Privacy" in the first week).

[227] Fed. Trade Comm'n, *FTC Gives Final Approval to Settlement with Google Over Buzz Rollout*, (Oct. 24, 2011), http://www.ftc.gov/opa/2011/10/buzz.shtm; Fed. Trade Comm'n, *Facebook Settles Charges That It Deceived Consumers by Failing to Keep Privacy Promises* (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm.

mind. Giving the service a name gives critics power over the thing named and the salience needed to support a messaging campaign.[228] It is much more difficult to launch a campaign against a privacy lurch with no name.

# III. BRANDING PRIVACY

If we are worried about the disruptive and potentially harmful force of dramatic, expectation-defying privacy lurches, we should consider using the law to tie privacy promises to trademarks and brands, an approach I am calling "branded privacy." Privacy law's principal difficulty is with endemic information-quality problems surrounding meaningful notice online. Trademarks are designed precisely to focus consumer attention on a particular set of important meanings.

The devil will be in the details, so this Part considers the details closely. Subpart A, after first presenting the proposal, connects theories of privacy and trademark and demonstrates how branded privacy can be well-supported by both. Next, subparts B and C discuss in detail the various shapes the proposal might take and how it might be implemented through common-law suits, the work of regulatory agencies, or new legislation. After presenting, in subpart D, examples of how branded privacy might work in action, the discussion concludes in subpart E by responding to likely objections.

## A. Tying Brands to Privacy Promises

I call the proposal "branded privacy." Policy makers should treat some of the data-handling decisions of almost every company as an immutable set of choices connected to the trademark the company has chosen for its product or service.[229] This connection should be set at the birth of the mark, and a company that later decides to abandon a promise of privacy it has made to it is customers should be forced to choose a new mark. The underlying logic of the proposal is that by shifting away from a central privacy promise, the company essentially creates, from the vantage point of consumer privacy, an entirely new service, one that cannot justifiably be associated with the goodwill attached to the older mark.[230] Google's consolidated user database, Facebook's default "visible to the Internet" setting, and Charter Communication's foray into behavioral advertising all represent business strategies that are different in kind—not simply in degree—from the business models they replaced. Users are entitled to be given clear, unambiguous notice of changes to privacy like these, but given the endemic information-quality problems online, the only effective way to deliver this is by leveraging the unique power of a trademark.

Although this prescription is novel—my research turned up no other proposal remotely similar to this one—it is not radical. It is well-supported by

---

[228] Compare the debate over the Carnivore FBI wiretapping technology. The technology still exists today, but now bears the much less menacing name DCS-1000, and it rarely gets mentioned in debates any more. Orin Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003).

[229] Once again, I am using the term "trademark" to refer to trademarks, service marks, and in some cases even to the more general term, "brand." *Supra* note 190.

[230] Grimmelmann, Saving Facebook, *supra* note 4, at 1201 ("[T]he initial design of the system is a representation to users that information they supply will be used in certain ways; by changing the service in a fundamental, privacy-breaching way, the site also breaches that implicit representation.").

many theories that have been advanced by scholars of both information privacy and branding. Consider the teachings of each field in turn.

1. Branded Privacy and Privacy Law Theory

Branded privacy sits comfortably within theories of information privacy law in at least three ways. First, it pushes companies to think deeply and consciously about their commitments to information privacy in the early stages of their lifecycles. Second, this rationale echoes motivations for "Privacy by Design,"[231] an influential new approach to privacy, but improves upon some of its shortcomings. Third, it continues the work of scholars trying to tie online privacy to consumer protection law, by finding a way to create effective warning labels for the Internet. Fourth, it might nudge companies finally to compete on privacy, a market whose absence many privacy scholars have long lamented.

a) Forcing Companies to Make Privacy Commitments

Branded privacy responds to the possibility that companies may embrace privacy lurches as intentional strategies by coaxing companies to commit themselves to fully specified and publicly revealed promises about the way they handle information at the time they launch their services to the public.[232] And once they make these commitments, they should feel strong regulatory pressure to stick with them.

Branded privacy thus recognizes that it is difficult for a company to "bolt on" privacy after the fact. We should encourage laws, regulations, and enforcement practices that nudge companies to think about privacy at birth, by weighing the pros (innovative new features) against the cons (threats of privacy harm to users) of any design decision. Branded privacy will not dictate whether a company should choose the privacy-enhancing or privacy-diminishing path, but it will bind them to their initial choices.

And after these choices are made, and companies announce them publicly, memorializing them, for example, in privacy policies, they will be treated like constitutional decisions, and they will stick. From that point forward, companies will be allowed to make small tweaks to minor information-handling policies. But plaintiffs and regulators will be able to treat any choice to change a core privacy commitment as an act of reconstitution, which would require more in the way of public notice and government compliance.

In order for branded privacy to work, companies must somehow be incentivized both to make concrete privacy commitments and to give the public notice of those commitments. Branded privacy might be gamed by companies that provide only muddled or vague promises of privacy, and likewise it will be defeated if companies delay making decisions about privacy issues.

It may be that if some regulatory body publicly embraces branded privacy—for example, if the FTC announces it will seek to enforce branded privacy[233]—this alone will serve an important new notice-forcing function. Given the severity of the rebranding remedy, companies might feel added pressure to declare their privacy commitments unambiguously and clearly at launch. Company executives will likely be terrified by the prospect of losing a

[231] PRIVACY BY DESIGN, http://privacybydesign.ca/ (last visited Mar. 18, 2012).

[232] I take for inspiration Tim Wu's recent proposal for a "constitutional approach to the information economy." TIM WU, THE MASTER SWITCH 304 (2010). Although the labels are similar, the concepts described are quite distinct.

[233] *Infra* Part III.C.2.

valuable brand, and the sheer possibility of such a fate might inspire them to make privacy commitments and to announce them loudly and unambiguously. At the very least, the remedy is likely to spur internal company deliberations about core privacy commitments and whether they should be revealed.

Regulators embracing branded privacy can augment this kind of notice forcing through rules and legal presumptions. For example, the FTC might announce that it will read privacy policies that are ambiguously or incompletely drafted to provide the maximum amount of privacy, at least for these purposes. In essence, this will operate in the spirit of the contract rule that ambiguities are interpreted against the drafter.[234] In such cases, later, clearer company announcements suggesting a less-privacy-protective policy will be seen as the kind of shift that subjects a company to the branded-privacy remedy.

Finally, Congress or the FTC might couple branded privacy with a rule that mandates clear, public, and unambiguous commitments about important privacy decisions. Think of it as a mandatory product labeling law for the Internet. Congress has already required this kind of notice forcing in sectoral privacy laws such as HIPAA and GLB, and the FTC has required clarity in some of its settlement orders resolving charges of unfair or deceptive trade practices. These might serve as models for a much more sweeping notice-forcing rule across industries, as a way to bolster a branded-privacy rule.

b) Giving Teeth to Privacy by Design

Branded privacy will both support and improve upon a growing movement in regulatory circles for what is called Privacy by Design.[235] Associated most closely with Ann Cavoukian, the Information and Privacy Commissioner for the Province of Ontario, Privacy by Design encourages companies to revamp their internal processes to better incorporate good privacy practices in initial design.[236] Privacy by Design touts seven "foundational principles," including, for example, "privacy as the default setting" and "privacy embedded into design."[237]

The first foundational principle of Privacy by Design is "proactive not reactive; preventative not remedial." Commissioner Cavoukian's office elaborates this principle in the following way:

> [Privacy by Design ("PbD")] anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred—it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

Privacy by Design, as currently elaborated, suffers from a few shortcomings that branded privacy can address. First, Privacy by Design focuses mostly on procedure and not substance. It says much about the need to revamp engineering design processes in order to push privacy consciousnesses down into the job descriptions of the working engineers, but it says too little about what it means by good privacy design. Second, Privacy by Design relies

---

[234] RESTATEMENT (SECOND) OF CONTRACTS § 206 (1981).

[235] *Id.*

[236] *Privacy by Design: From Policy to Practice*, PRIVACY BY DESIGN (Sept. 2011), http://privacybydesign.ca/content/uploads/2011/09/pbd-policy-practice-aug10.pdf.

[237] Ann Cavoukian, *The 7 Foundational Principles*, PRIVACY BY DESIGN (Aug. 2009), http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

mostly on voluntary implementation by companies, albeit sometimes with the participation of a regulator, perhaps through what some have called "regulation by raised eyebrow."[238] The problem is that even when privacy is baked into a product or service, it can be unraveled easily, so Privacy by Design should do more to recognize the great temptations companies feel to sacrifice user privacy for profits. Third, although Privacy by Design touts the importance of transparency, it remains vague about how transparency should be implemented.[239]

Branded privacy addresses every one of these shortcomings, giving a firmer base for the idea. In any implementation of branded privacy, companies will need to commit themselves to specific core privacy decisions. Then, once selected, they will be obligated to publicly list the choices they have made, advancing Privacy by Design's transparency principle. Most importantly, faced with the risk of losing a valuable brand name, companies are much more likely to adhere to their initial choices than under a purely voluntary regime.

c) Better Notice: Warning Labels for the Internet

James Grimmelmann notes the "natural affinity between the privacy law challenges facing Facebook and . . . product safety" law.[240] Building on the work of others, he develops parallels between privacy and product safety, expanding familiar tort principles to online privacy problems.[241]

Most importantly, he wonders whether we might cure some of the problems with notice and choice by borrowing tort law's encouragement of the use of warning labels.[242] "A good warning can point out hidden dangers to help a user avoid them or even make an informed decision to avoid the product entirely."[243] This seems especially important to alert users to unexpected change.[244]

Sudden, unanticipated, invisible changes to data handling practices bear more-than-passing resemblance to the kind of harms that we use product safety law to help prevent. According to the Restatement (Third) of Torts: Products Liability, a product that injures subjects a producer to liability "because of inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings."[245]

---

[238] Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. DAVIS L. REV. 529, 559 (2009). As an example of the way companies can work with regulators to implement Privacy by Design together, consider the paper about bringing the principle to the smart grid jointly authored by the Privacy Commissioner of Ontario and San Diego Gas and Electric. SDG&E, SDG&E Launches Smart Grid Privacy Initiative (March 8, 2012), http://sdge.com/newsroom/press-releases/2012-03-08/sdge-launches-smart-grid-privacy-initiative.

[239] Cavoukian, *supra* note 237, at 2 (listing principle six: "visibility and transparency").

[240] Grimmelmann, *Product Safety*, *supra* note 16 at 813.

[241] *Id.*

[242] *Id.*

[243] *Id.*

[244] *Id.*

[245] RESTATEMENT (THIRD) OF TORT: PROD. LIAB. § 2(c) (1998).

In product safety, warning labels must be placed in conspicuous places, likely to be seen just at the moment the risky behavior commences.[246] Brightly colored labels are often attached directly to the power cord of a hair dryer or toaster, reminding the consumer about the risk of electrocution near water.

What is the power cord of a web? Often the risk to privacy stems directly from the use of a website itself, so the digital warning label should be posted somewhere conspicuous on the page itself. For this reason, California requires a link with the words "privacy policy" to appear somewhere on the first webpage visited.[247] Courts construing online contracts have gone further, parsing a website into different parts, some more conspicuous than others. In *Specht v. Netscape Communications Corporation*, a court refused to give effect to contract terms that were revealed only to consumers who knew to scroll down the page before clicking the agreement button.[248] The FTC issued a report entitled *Dot Com Disclosures* providing similar advice.[249]

For some subcategories of online risk, such as the risks from behavioral, visual (as opposed to purely textual) advertising, the web does have a power-cord equivalent, the ad itself. In 2010, two advertising industry groups, the Interactive Advertising Bureau (IAB) and Network Advertising Initiative (NAI) voluntarily agreed to place explanatory icons directly on targeted ads to warn consumers about the targeting being used.[250]

But most other online interactions lack such an obvious place to place an online warning label. Since no standardized warning label for the Internet has been embraced, companies devise their own methods of alerting consumers to change, often by posting open letters or blog posts to their customers full of the doublespeak described earlier.[251] We can do better. We need to find warning labels for the Internet that are not so susceptible to doublespeak. We need to find a concise, compact form of information that alerts the consumer to the heightened risk to privacy, without engendering the kind of confusion and ambiguity so typically witnessed today.

On the Internet, often the trademark itself (whether displayed as text in the browser's title bar or designed into the conspicuous logo pasted to the top of every page) sits perhaps on the only place where an effective warning label can appear. No other place on a website is as likely to be seen and noticed, particularly given recent trends in technology away from desktop computers and toward smart phones and tablet computers, which mean more

---

[246] *See* Wilson Foods Corp. v. Turner, 218 Ga. App. 74, 75 (Ct. App. Ga. 1995) ("Failure to communicate an adequate warning involves such questions, as are here at issue, as to location and presentation of the warning.").

[247] CAL. BUS & PROF. CODE §§ 22575, 22577 (West 2004).

[248] 306 F.3d 17(2d Cir. 2002).

[249] FED. TRADE COMM'N, DOT COM DISCLOSURES: INFORMATION ABOUT ONLINE ADVERTISING (2000), available at http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf [hereinafter DOT COM DISCLOSURES].

[250] *IAB and NAI Release Technical Specifications for Enhanced Notice to Consumers for Online Behavioral Advertising*, INTERACTIVE ADVERTISING BUREAU (April 14, 2010), http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-041410. *Cf.* DOT COM DISCLOSURES, *supra* note 249, at 1 ("In evaluating whether disclosures are likely to be clear and conspicuous in online ads, advertisers should consider the *placement* of the disclosure in an ad and its *proximity* to the relevant claim." (emphasis in original)).

[251] *Supra* Part II.A.3.c.

users than ever view websites on small screens. With screen real estate at a premium, many websites produce scaled-back, mobile versions on which only the most essential information can appear.[252] Large, conspicuous warning labels are not compatible with this medium.[253]

d) Creating a Market for Privacy

Once we implement branded privacy, we will force companies to make and publicize their privacy commitments and connect those commitments to their brands. This, in turn, will likely push companies to separate themselves into two camps enacting diametrically opposed strategies, perhaps leaving no companies sitting in between: some companies will decide to compete aggressively on privacy and thus promise robust forms of privacy at launch. Other companies, deciding that robust privacy is not for them, will be driven to the other extreme, crafting privacy policies that leave open the possibility of any shift whatsoever for all time. Companies will be unlikely to strike out middle positions, offering some but not too much privacy, because they will lose the public relations benefits of choosing to be private but also lose the flexibility of choosing to be anti-private. Companies will know that such a position will leave them flanked by competitors on both sides with structural market advantages they will not enjoy.[254]

Some might complain about this result, arguing that the tendency for branded privacy to lead to two and only two distinct types of privacy actors meddles too much with a free market. A rule that tends to push companies into a bimodal distribution along the privacy axis will seem to sap the vitality and product differentiation that is so important in a healthy market and also so much a part of the history of the evolution of the Internet.

I see things differently. This criticism points to "a feature, not a bug."[255] Ever since legal scholars began taking up the issue of privacy on the Internet, they have bemoaned the fact that individuals never seem to express their privacy preferences in the market.[256] "There is no market for privacy," many have complained.[257] I think part of the problem is the murky market

---

[252] *See* Andrea Matwyshyn, *Resilience: Building Better Users and Fair Trade Practices in Information*, 63 FED. COMM. L.J. 391, 407 (2010) ("The task of reading multiple cross-referenced linked documents, potentially on a small mobile device, is limiting, at best. At worst, it is taking advantage of a crippled user interface."); FTC FINAL REPORT, *supra* note 176, at 63–64. (noting the "small space available for disclosures on mobile screens").

[253] *See* J. Scott Ducher, Note, *Caution: This Superman Suit will not Enable You to Fly—Are Consumer Product Warning Labels out of Control?*, 38 ARIZ. ST. L.J. 633, 655 n.177 (2006) (describing author's hunt for iPod warning about potential dangers to hearing).

[254] Game theoreticians might model the publication of privacy policies in pursuit of customers as a "signaling game," *See* ERIC A. POSNER, LAW AND SOCIAL NORMS 34 (2000). The signaling game for privacy seems ordinarily to lead to a semi-pooled equilibrium, but branded privacy will push it to a separating equilibrium instead. *Id.* at 19, 25.

[255] The Jargon File, Feature, http://www.jargon.net/jargonfile/f/feature.html.

[256] *E.g.* Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 763–71 (2000) (explaining the failure of a market for privacy).

[257] *E.g.* Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191, 236 (2011) ("If a healthy market for privacy existed, consumers would be able to vote with their dollars.")

for privacy online. Every website promises privacy yet few deliver. Privacy seems to be a market for lemons where promises are easy to make and quality is difficult to inspect.[258] As with all such markets, there seems to be little incentive to compete for privacy.

But things would change if firms began separating themselves into two separate piles. The full-privacy firms would say, "use us, we are private," while the non-privacy firms would argue, "we might not be very private, but look at the services we offer!" If this happens often enough, consumers might learn to trust the content and stability of the different signals they are being sent, and a market for privacy just might emerge as a result.

### 2. Branded Privacy and Trademark Law Theory

#### a) Traditional Trademark Theory and Source Identification

According to traditional trademark theory, producers use trademarks to convey information about the source of a good or service. Indeed, many argue that source identification is the only form of communication protected under traditional trademark law.[259] These traditional theories are built almost entirely upon a law and economics theory about search costs.[260] The law protects trademark users from confusingly similar uses by free-riding competitors, because in so doing, it lowers consumer search costs, incentivizing and justifying investments in quality control, enhancing overall economic efficiency.[261]

Seen through the traditional law and economics lens, trademark theory provides little support for branded privacy. My claim is not that consumers become confused during a privacy lurch about the source of the service offered; instead, they misunderstand the qualities of the service they long ago signed up to use. In addition, traditional trademark theory and law focuses almost entirely on clashes between competitors—the paradigmatic trademark lawsuit involves a senior user and a late-arriving junior user fighting over the collision of their two marks. Branded privacy focuses instead on a single company's abrupt change, whether or not it clashes with the actions of competitors.

#### b) Traditional Trademark Theory and Quality Control

Although traditional trademark theory provides little support for branded privacy, well-established pockets of trademark law doctrine and scholarship support directly the idea that trademark law should prevent producers from disrupting consumer expectations about the quality they come to expect from trademarked products and services. Admittedly, these

---

[258] Tony Vila et al., *Why We Can't Be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market*, HARVARD UNIVERSITY (May 15, 2003), *available at* http://www.eecs.harvard.edu/~greenie/econprivacy.pdf; Joseph Bonneau & Soren Preibusch, *The Privacy Jungle: On the Market for Data Protection in Social Networks*, in 2010 ECONOMICS OF INFORMATION SECURITY AND PRIVACY (Tyler Moore et al. eds., 2010) 159–60 ("The market for privacy in social networks also fits the model of a lemons market well . . . ."); George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 492–94 (1970).

[259] *Supra* note 204.

[260] Beebe, *supra* note 13, at 623-24 ("The influence of [the law and economics justification for trademark] is now nearly total. It has been adopted at the highest levels of American law. No alternative account of trademark doctrine currently exists.").

[261] Landes & Posner, *supra* note 192, at 269-70.

pockets are sometimes viewed as outliers by scholars, rules that fit poorly within orthodox trademark theory.

Trademark scholars and judges have long referred to the role trademarks play in guaranteeing consistent quality.[262] The entire point of trademark law is that consumers will select a familiarly marked product over one bearing an unfamiliar mark, calculating that the marked product will promise a consistent baseline of some quality they value, such as taste or durability.[263] This idea has led to the formalized model of "goodwill," the label given to the positive feelings consumers have for the products or services sold by a particular company or under a particular brand.[264]

To be clear, most scholars see quality assurance and goodwill as the end states or by-products of trademark law, not as essential qualities the law must bend to ensure.[265] The verb often used to describe the relationship between trademark law and quality control is "encourage": "When it works well, trademark law facilitates the workings of modern markets by permitting producers to accurately communicate information about the quality of their products to buyers, thereby *encouraging* them to invest in making quality products . . . ."[266] Because certain uses by competitors of a mark are forbidden, consumers will begin to expect quality, and not the other way around.

In fact, experts are quick to point out that trademarks are protectable even attached to low-quality goods.[267] More often, however, the promise of enforceable trademarks and protectable goodwill encourages at least a modicum of quality control, through what some have called the "self-enforcing" nature of trademarks.[268] According to Landes and Posner, "[t]he benefits of trademarks in reducing consumer search costs require that the producer of a trademarked good maintain a consistent quality over time and across consumers. Hence trademark protection encourages expenditures on quality."[269] The self-enforcing quality control mechanism no doubt plays a role in privacy, as companies like Google, Facebook, and Twitter know that consumers associate their brands with particular types of privacy promises.[270] They also know how trademarks can punish a company stigmatized (fairly or not) with

---

[262] *E.g.,* Park 'N Fly, Inc. v. Dollar Park & Fly, Inc., 469 U.S. 189, xx (1985) ("[T]rademarks desirably promote competition and the maintenance of product quality.").

[263] MCCARTHY, *supra* note 206, at § 2:4 ("[T]rademarks create an incentive to keep up a good reputation for a predictable quality of goods.").

[264] Robert G. Bone, *Hunting Goodwill: A History of the Concept of Goodwill in Trademark Law*, 86 B.U.L. REV. 547 (2006).

[265] *Id.* at 556 n.27 ("The point is not that trademark law provides affirmative incentives to improve quality. . . . Trademark simply assures that when a firm creates a higher quality product . . . it is able to communicate that fact to consumers.").

[266] Mark A. Lemley & Mark McKenna, *Irrelevant Confusion*, 62 STAN. L. REV. 413, 414 (2010) (emphasis added).

[267] MCCARTHY, *supra* note 206, at § 3:10 ("It is important to note that the quality function of marks does not mean that marks always signify "high" quality goods or services—merely that the quality level, whatever it is, will remain consistent and predictable among all goods or services supplied under the mark.").

[268] Landes and Posner, *supra* note 192, at 270.

[269] *Id.*

[270] *See* MCCARTHY, *supra* note 206, at § 2:4 ("[G]oods of uniformly poor quality soon disappear from the market. A maker of a shoddy product can only fool some of the people some of the time.").

a reputation for poor privacy practices; they need only look to examples like Acxiom,[271] NebuAd,[272] or CarrierIQ[273] for that.

This purist's vision of trademark, which views consistent quality as a by-product and not a value directly policed by trademark law, runs headlong into pockets of trademark doctrine it cannot explain. Several well-established rules penalize mark holders for failing to maintain particular levels of quality. A trademark can be lost through abandonment, which happens when a trademark owner ceases using the mark without intent to resume.[274] Assignment of a trademark "in gross," meaning without the associated goodwill, can similarly lead to the loss of trademark rights.[275] Licensors can lose trademark rights when they fail to supervise the quality control of licensees, sometimes called naked licensing.[276] These rules push companies to work to maintain consumer associations between trademarks and the quality of their products to retain the benefit of the law.[277]

A related set of cases, what some call the "rebuilt product cases," use trademark law to force consistent quality.[278] These cases ask whether a purchaser of a trademarked good can resell the product using the original brand, despite having made repairs to it. In other words, when are repairs so fundamental to the quality of the resold product that it would cause confusion to the consumer to allow it to be sold with the original brand? For example, when is a rebuilt luxury watch[279] or a reconditioned spark plug[280] so different in its qualities that the trademark holder deserves a remedy enjoining use of its mark? Laura Heymann synthesizes these cases into an "essential qualities" test.[281] In some cases, a defendant might "alter[] the good's essential qualities such that the trademark . . . can no longer be said to denote the same good."[282] These cases, although sitting outside the central stream of trademark theory, have a long pedigree.

Professor Heymann provides a useful vocabulary for distinguishing all of these rules from the traditional, source-identification rules from which they depart, borrowing from linguistic and philosophical studies of naming.[283] Rules focused only on source identification recognize and enforce the denotative function of naming. Names "provide a shorthand for an entity that can be

---

[271] Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERK. BUS. L.J. 129, 196-203 (2005) (discussing Acxiom's business model and security lapses).

[272] *Supra* Part I.B.2.

[273] Andy Greenberg, *Phone 'Rootkit' Maker Carrier IQ May Have Violated Wiretap Law in Millions of Cases*, FORBES.COM, Nov. 30, 2011, http://www.forbes.com/sites/andygreenberg/2011/11/30/phone-rootkit-carrier-iq-may-have-violated-wiretap-law-in-millions-of-cases/ (quoting author of Article).

[274] Emergency One, Inc. v. American FireEagle, Ltd., 228 F.3d 531 (4th Cir. 2000).

[275] Marshak v. Green, 746 F.2d 927 (2d Cir. 1984).

[276] Barcamerica Intern. USA Trust v. Tyfield Importers, Inc., 289 F.3d 589 (9th Cir. 2002).

[277] Some scholars argue for the abolishment of quality control requirements like these. Irene Calboli, *The Sunset of "Quality Control" In Modern Trademark Licensing*, 57 AM. U.L. REV. 341, 377-78 (2007) (arguing that changes to market structure threatens modern licensing practices, which, in turn, have become "fundamental pillar[s] of the economy").

[278] Heymann, *supra* note 209, at 423-28.

[279] Cartier, Inc. v. Symbolix, Inc., 386 F. Supp. 2d 354 (S.D.N.Y. 2005).

[280] Champion Spark Plug Co. v. Sanders, 331 U.S. 125 (1947).

[281] *Id.* at 425.

[282] *Id.*

[283] *Id.* at 391-93.

used by others as a reference."[284] Other rules, like trademark abandonment, protect instead the connotative function of naming,[285] Names "communicate, either directly or by suggestion, certain characteristics about a person or good, whether actual or aspirational."[286]

The idea that trademark law recognizes the connotative function of trademarks and is connected to stability and constancy suggests a conflict with the rise of the pivot and the privacy lurch. When a company uses a single symbol, logo, or name to refer to a music sharing site one day and a cloud storage site the next, it might no longer deserve the full benefit of trademark law.

This argument earns support once we consider the strategic tendencies of modern companies. In the past, companies would sometimes vary trademarks in order to signal even subtle changes to their consumers, rather than risk losing the goodwill they had so carefully built up. In 1985, a prominent and successful corporate giant made something like this pitch to consumers: This Coke tastes different, maybe for the better and maybe for the worse, not because our quality control measures have changed, but because it's actually 'New Coke,' a different product altogether.[287] We think it is better, and if you agree, we will probably drop the 'New' signifier in a year or two, but for now, we are hedging our bets in case you disagree and dislike the new offering.[288] This turned out to be a wise calculation.[289]

Today's companies seem to invert this strategy. Trademarks are used to obscure rather than highlight change. Today's consumer "non-pitch" sounds more like this: This service is actually quite different from the service you originally signed up to use, and the changes mostly benefit us and might even harm you. But if we alerted you to this change, for example by adding "New" to our brand, we might lose you. By keeping the old name and old look-and-feel of the service, companies are trying to make potentially important changes seem unimportant and unworthy of scrutiny. This is trademark as smokescreen for change rather than as signifier of quality. This might stretch trademark law too far.

### c) The New Trademark

It might be enough to build support for branded privacy upon a foundation of the quality control ideas sprinkled throughout trademark doctrine. If we combine the motivations behind the rules against assignment in gross

---

[284] *Id.* at 392.

[285] *Id.*

[286] *Id.* Professor Heymann is not comfortable with rules in trademark law that seek to protect "nonessential changes" or "emotional connotations" in rebranding. *Id.* at 386. But she does not criticize rules focused on connotative meaning about essential changes. In Part III, I will argue that some privacy changes should qualify within this meaning of essential.

[287] *See* Irene Calboli, *The Sunset of "Quality Control" in Modern Trademark Licensing*, 57 AM. U.L. REV. 341, 391 n.300 (2007) (discussing Coca-Cola's ill-fated and short-lived switch to "New Coke" brand).

[288] Aaron Perzanowski provides another example. Starbucks has begun experimenting with "stealth stores" around Seattle through which they are experimenting with new business models. They are using different names—for example 15th Avenue Coffee & Tea—to perform the experiment. Aaron Perzanowski, *Unbranding, Confusion, and Deception*, 24 HARV. J.L. & TECH. 1, 14-15 (2010)..

[289] The Coca-Cola Co., *Coke Lore: The Real Story of New Coke*, http://www.thecoca-colacompany.com/heritage/cokelore_newcoke.html (last visited March 29, 2012) (describing the rise and eventual fall of New Coke).

and naked licenses, with the logic of the rebuilt products cases, and with the way economic theories of trademark tend to encourage stability and high quality, and if we tilt our head, just so, as we look at this Frankensteinian combination we might see a sketchy, theoretical basis for branded privacy. But this would be both unsatisfying and slightly disingenuous, as most of the strands of theory and doctrine recited in the previous Subpart are seen as aberrations, waiting to be pruned from trademark law by the shears of time.[290]

It is better instead to confess that branded privacy represents something new, an expansion of traditional thinking about brands and trademarks, a theory that sits outside trademark law's traditional core, a theory about trademarks (and brands) but not exactly about trademark law. But although this theory may be new, it finds many fellow travelers, direct support in the work of a number of scholars who have very recently, only in the past five years, begun to invert the focus of trademark theory: where most scholars see trademarks as weapons wielded by senior users against competitors, to protect either the interests of consumers or their own intangible property, a new wave of scholarship casts trademarks instead as weapons to be wielded against the trademark holders themselves to protect consumer interests. To date, most of these scholars have failed to draw the connections between one another, to recognize the way they have been launching what I will call "The New Trademark."[291]

Shahar Dillbary provides a cornerstone of the New Trademark, with his work advocating "intra-brand" policing of trademarks, going beyond the "inter-brand" policing of traditional trademark infringement and dilution claims.[292] Dillbary's work focuses on how trademarks can function as communicative devices to mislead, deceive, or treat consumers unfairly.[293] He calls, for example, for an expanded use of false advertising laws to prevent companies from reformulating their marked goods and services.[294] Like other New Trademark theorists, Dillbary does not claim to be writing about trademark *law* at all, rather he is calling for new private causes of action or theories of agency enforcement that let us focus on the special harms associated with intra-brand abuses.

Another New Trademark building block is Aaron Perzanowski's article on "unbranding," the name he uses to describe the act of intentionally abandoning a trademark after a quality control problem.[295] As examples he cites Comcast's decision to rebrand its consumer-facing service to Xfinity to clean the slate on its poor consumer service reputation; ValueJet becoming AirTran after a tragic 1996 crash; and Philip Morris's rebranding as Altria to ease the stigma the company felt from its history selling cigarettes.[296] Perzanowski argues that the FTC can, and should, act to prevent deceptive examples of unbranding. A student note in the Harvard Law Review proposed a similar solution, arguing that companies that accumulate negative

[290] Calboli, *supra* note 287.
[291] With apologies to Paul M. Schwartz & William Michael Treanor, *The New Privacy*, 101 MICH. L. REV. 2163 (2003), and Charles A. Reich, *The New Property*, 73 YALE L.J. 733 (1964).
[292] Dillbary, *supra* note 200; J. Shahar Dillbary, Trademarks as a Media for False Advertising , 32 Cardozo L. Rev. 327, 328 (2009).
[293] *Id.*
[294] *Id.*
[295] Aaron Perzanowski, *Unbranding, Confusion, and Deception*, 24 HARV. J.L. & TECH. 1 (2010).
[296] *Id.* at 2, 11.

associations with a mark, badwill, should be required to keep the mark for some time, to avoid consumer confusion and harm.[297]

To broaden the New Trademark cohort beyond scholars trying to police intra-brand uses of trademarks, we can add others focused on brands more broadly. Deven Desai has criticized traditional trademark approaches as "blinkered and confused,"[298] missing "[t]he noncorporate dimension of branding [which] involves consumers and communities as stakeholders in brands."[299] Desai argues that the parallel corporate dimension to branding helps explain many of the last half century's expansion of trademark law, but without embracing noncorporate interests, the "brand theory" of trademark is as-yet incomplete.[300]

Under his brand theory approach, Desai would have the law recognize the "shared value"[301] approach to brand development. He connects this argument directly to work by other scholars in law and media studies chronicling the rise of antibranding or culture jamming.[302] Desai implies that courts focused on brand theory should sometimes decline to enjoin uses of brands by consumers and communities in cases that would turn out the other way under traditional approaches. It is perhaps a small step to use Desai's brand theory to support intrabrand enforcement of trademarks. We can shape the kind of healthy brand dialectic Desai desires by cabining the worst, most deceptive forms of brand redefinition.

What joins the New Trademark scholars is a willingness to look beyond economic theories for support.[303] They build upon, for example, those theorists have tried to tie trademark law to a liberal theory account of human autonomy,[304] or to free expression.[305]

By looking beyond the bare efficiency frame of law and economics, we can find further support for the branded privacy solution. For example, non-economic theories account better for arguments about power and control. We might begin to see rebranding as a way to equalize power imbalances in society. This dovetails once again with Professor Heymann's work on naming, as names are often intertwined with power.[306] In Genesis, God gave Adam the power to name all of the animals.[307] Throughout history, governments and other powerful entities have used the power to name as a way to control another class of individuals, often including persecuted and oppressed classes of people.[308]

I am drawing a line around disparate scholars, some of whom might disagree with the prescriptions made by others in the group. In fact, some or

---

[297] Note, *Badwill*, 116 HARV. L. REV. 1845 (2003).
[298] Deven R. Desai, *From Trademarks to Brands*, 64 FLA. L. REV. 981, 981 (2012).
[299] *Id.* at 986.
[300] *Id.* at 1036-37.
[301] *Id.* at 1042.
[302] NAOMI KLEIN, NO LOGO (2002); Sonia K. Katyal, *Stealth Marketing and Antibranding: The Love That Dare Not Speak Its Name*, 58 BUFFALO L. REV. 795 (2010).
[303] *Cf.* Mark P. McKenna, *The Normative Foundations of Trademark Law*, 82 NOTRE DAME L. REV. 1838, 1844 (2007) (arguing that the history of trademark law belies a close connection to economic efficiency rationales).
[304] Dillbary, *supra* note 200.
[305] Laura A. Heymann, *The Public's Domain in Trademark Law: A First Amendment Theory of the Consumer*, 43 GA. L. REV. 651, 667-97 (2009).
[306] Heymann, *supra* note 209, at 406-07.
[307] *Genesis* 2:19 (King James).
[308] Heymann, *supra* note 209, at 407 n.98 and text accompanying.

all of these scholars might disagree with my branded privacy prescription, which in some ways go further than any of the others. The point is not that these scholars deserve to be unified as carriers of the same banner or practitioners of a single theory; this is a looser coalition of scholarship than that. What every one of these theories has in common is the idea that trademarks need sometimes to be treated as a two-way street. Because of the information qualities of these essential marketplace symbols, we need to police the way trademarks are used by the senior users, as much as we have policed uses by junior users. These theories seek to take back from trademark holders, in the name of preventing deception and other harm, a little of what trademark law has given away for centuries.[309] All of these theories, and branded privacy included, begin to reimagine trademarks, at least a little, as levers to be pulled by litigants and policymakers to serve the goal of consumer protection.

## B. The Details

Before we can weigh the benefits to notice (and ultimately privacy) of this solution against the costs to values like innovation, we need to spell out the variations on this idea that will set the pros and cons of the balance struck. There are at least four important variables to consider: (1) which privacy promises should trigger the requirement for a new brand; (2) whether or not companies should be allowed to migrate their users without consent to the new service, which corresponds to the traditional debate over opt-in and opt-out choice regimes; (3) what form the new brand should take and how much it must differ from the parent brand; and (4) how long the new brand should last. By varying these four properties, different regulators in different situations will be able to devise very different versions of branded privacy. For the most part, this Article remains agnostic about these choices. Some permutations will give the regulation more teeth while others will provide a lighter touch, disrupting market forces less.

### 1. Which Promises Should Be Bound?

The first and likely most important decision a legislator or regulator needs to make about branded privacy is to identify the set of promises that trigger the obligation to shift to a new brand.[310] I have referred repeatedly so far to the "core set of privacy promises" that trigger the rebranding remedy when breached, but what belongs on that list? If the list of triggers is long or full of vaguely defined standards, critics will complain that the rule unduly burdens market forces. On the other hand, if the trigger list is too narrowly defined, the benefit to privacy will be slight.

Along the spectrum from long and overbroad to short and underprotective, we should be mindful of the novel and aggressive nature of the prescription. Brands are important tools of consumer protection and markers of accumulated business goodwill, and we should be hesitant to disrupt them spuriously. At the same time, these same characteristics of brands explain why this tool promises such robust privacy protection.

---

[309] *Id.* at 56 (arguing for a change to trademark law that "reorients and revives the role of trademarks as true information resources, not simply one-way tools controlled by corporations").

[310] The FTC refers to this as the question of materiality. FTC PRIVACY REPORT, *supra* note 151, at 77 (seeking "comment on the types of changes companies make to their policies and practices and what types of changes they regard as material"); FTC, ONLINE BEHAVIORAL ADVERTISING, *supra* note 8, at 41 n.73 and accompanying text (defining "material" and "material change").

We must also keep in mind the twin goals of this proposal: improving the information environment around privacy choice and enhancing stability and predictability for consumers and companies alike. Both goals would be defeated if we linked a long and cluttered list of privacy promises to the rebranding treatment. "Sensible policy would focus on encouraging [companies like] Facebook to make salient a few truly important facts about how it works, with good contextual help for the rest."[311]

a) Characteristics for Appropriate Triggers

The appropriate trigger list for the rebranding remedy of branded privacy will depend on the context, and individual regulators might promulgate multiple lists for different situations. Before considering specific candidate triggers, it will be helpful to survey the problem from a higher elevation, enumerating the characteristics of a proper trigger.

In describing these characteristics, I will refer repeatedly to the Fair Information Practice Principles, or FIPPs, described above.[312] These are a natural starting place, as scholars and regulators have debated these principles for more than forty years. Most widely-accepted examples of good privacy practices are included in some version of the FIPPs.

Characteristic One: Predictable. Given the aggressive nature of branded privacy, we should opt for predictability. In the jurisprudence literature on rules versus standards, many have concluded that rules provide ex ante certainty at the expense of some ex post fairness, which in turn is better advanced better by standards.[313] In this case, we should tend to select rules, because certainty is paramount; companies should not lose their brands in response to decisions that they could not have anticipated ahead of time. In other words, the point of branded privacy is to change incentives, not punish misbehavior, and the rules should be designed with that goal in mind.

Characteristic Two: Connected to Privacy Harm. Not every FIPP counteracts privacy harm directly. Some act more like due-process rights in data that set the proper environment for privacy, acting indirectly and prophylatically. For example, a FIPP included in almost every list is the principle of security.[314] Companies that fail to provide adequate security leave customer data susceptible to falling into the wrong hands through breach or hack. Although this is an important principle, it is too prophylactic to deserve to trigger branded privacy.

In addition, a brand should not be lost simply because a company tweaks a minor privacy setting. Instead, brand linkage should be made only for those privacy commitments we consider so essential, so fundamental to privacy, or so likely to raise significantly the risk of privacy harm that we include it on the list of choices that affix to a given brand.

Characteristic Three: Measurable. One way to advance the goals of predictability and certainty is to choose triggers that are quantifiable and measureable. Many FIPPs can be reduced to rough metrics. For example, data minimization focuses on the amount of information stored and the length of time for which it is stored.[315] Use limitation (tied closely to purpose specification) can be tied to number of third parties with which the data is

[311] Grimmelmann, *Product Safety*, *supra* note 16, at 822.
[312] *Supra* Part II.A.2.
[313] Pierre J. Schlag, *Rules and Standards*, 33 UCLA L. REV. 379 (1985).
[314] Gellman, *supra* note 148.
[315] *See* Soghoian, *supra* note 3, at 209–15 (discussing data retention time limits).

shared or spread within a single entity of the data. In both cases, we can test compliance simply by counting things.

A related quality for a good trigger is external observability. Some privacy practices are very hard to assess without invasive audits. Security is once again an example. Others, such as those that relate to how data flows with third parties outside a company, can sometimes be measured completely externally. For example, in online environments like the web and cell phones, third-party information often flows through third-party cookies, which can be observed by the consumer herself, without any participation from the companies being studied.[316]

Characteristic Four: Consistent with Prevailing Regulatory Traditions. Finally, triggers should be consistent with the prevailing regulatory traditions in a jurisdiction. This is less about ideal privacy policy and more an acknowledgement of political reality. Policymakers are much more likely to embrace branded privacy if they see it as strengthening legacy approaches rather than extending privacy policy into new areas. Thus, for example, the FIPP of Individual Participation, which provides individuals the right to examine information stored about them and correct incorrect information,[317] is rarely implemented in American privacy law.[318] Given this history, it would probably be asking too much of American regulators create new and somewhat foreign substantive rights while at the same time enforcing those rights in this aggressive new way.

b) Which Triggers?

Taking these characteristics into account, three FIPPs seem best able to serve as triggers: Collection Limitation,[319] Purpose Specification, and Use Limitation. All three involve directly controlling the flow of information in ways that minimize direct harm and find a long tradition of regulation in the United States in laws like HIPAA[320] and GLB[321].

All three lend themselves, at least imperfectly, to reduction to a metric. For example, according to the Use Limitation principle, as articulated by the OECD, "[p]ersonal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with [the

[316] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010 5:59 PM), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html

[317] Organisation for Economic Co-operation and Development, *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* O.E.C.D. Doc. C58 (final)(Oct. 1, 1980), *reprinted in* 20 I.L.M. 422 (1981), *available at* http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html#recommendation.

[318] The exception being the rights extended in the Privacy Act, which applies to "systems of records" held by the government. 5 U.S.C. § 552a. The Act provides individuals the right to review and request amendments to records about themselves. *Id.*

[319] The DHS's FIPP of "Data Minimization," which differs from Collection Limitation in some ways, belongs on this list as well. Dep't of Homeland Sec., Privacy Policy Guidance Memo.: The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[320] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.A.).

[321] Gramm-Leach-Biley Act, Pub. L. 106-102, 113 Stat. 1338 (enacted in 1999, codified in scattered sections of 12 U.S.C. and 15 U.S.C.)

Purpose Specification] principle" without consent.[322] This translates roughly to the idea that flows of information should not expand significantly to new third parties. If a company shares information with five third parties at the time a privacy promise is first made and at some future time expands to sharing with five hundred third parties (either suddenly or through a series of smaller shifts), this breaches the Use Limitation principle.

Other metrics can measure adherence to the Use Limitation principle in this rough way. Regulators might trigger brand reassignment any time a company dramatically increases: the number of people within a company who can access data; the number of databases to which a particular set of consumer data connects; or the length of time data is retained. This by no means exhausts the possible triggers for branded privacy, but the metrics discussed so far are likely to be included in most trigger lists.

Finally, if a company's new, post-lurch behavior would be prohibited by another privacy law, this too should trigger rebranding. This should be so even if the conduct is technically legal under an exception for user consent, because branded privacy assumes that information-quality problems plague opportunities for meaningful consent without better forms of notice. For example, cable companies embracing NebuAd and Phorm may have violated the Federal Wiretap Act, despite that law's exception for the conduct with consent.[323] As another example, Netflix might have violated the Video Privacy Protection Act when it released records reflecting the movies its users had rated as part of the Netflix prize.[324] In both cases, the companies relied on strained theories of consent.[325] But because both cases involved significant privacy lurches that fell within live prohibitions, regulators might have enforced branded privacy in either case.

c) One Specific Trigger: The Choice Not to Advertise

Given the organizing goal of predictability, it is probably not enough to recite the three FIPPs listed above, as the FIPPs are notoriously vague, jargon-laden, and subject to competing interpretations. The goal of a regulator promulgating a new rule of branded privacy should be to define triggers much more concretely and plainly. For example, rather than announcing the trigger of "Use Limitation," a regulator should instead announce that one trigger measures the change in the number of people inside the company who can access the data.

Another way to make the FIPPs much more concrete is to create triggers that are tied to commonly encountered scenarios or purposes. One example seems so commonly a part of the most worrisome privacy lurches that it deserves specific discussion: a company's decision to switch for the first time to a behavioral-advertising model. Companies that do not sell user information to advertisers at birth should not be allowed to sell user information for this purpose later unless they select a new brand. This is a fairly straightforward application of the FIPPs of Purpose Specification and Use Limitation but one given teeth by branded privacy. Consider a few examples.

When cable broadband providers, like Charter Communications, partnered with NebuAd to begin selling ads based on customer web-surfing

[322] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data , 23 September 1980, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
[323] Ohm, *Rise and Fall, supra* note 51.
[324] Ohm, *Broken Promises*, *supra* note 93.
[325] *Id.;* Ohm, *Rise and Fall, supra* note 51.

habits, they abandoned decades of past practice in favor of an egregious lurch toward advertising.[326] Given this dramatic and unprecedented shift, and especially given the sensitivity of the information Charter was positioned to watch,[327] this service should not have been permitted without a new brand.

As another example, consider an even older group of incumbents, the nation's many electrical power companies. These companies have been building the so-called smart grid, integrating information and communications technology into the legacy power grid, in order to reveal fine detail about energy usage in homes and businesses, through technologies like smart meters.[328] Proponents tout the way the smart grid will revolutionize grid operation, paving the way for significant new efficiencies.[329] They also highlight how the fine-grained detail they are generating about energy usage in the home will lead to greater consumer awareness and, ultimately, assist conservation efforts.[330]

But the smart grid has also given rise to entirely new markets for entrepreneurs who imagine new applications that take advantage of all of this new data about consumer habits.[331] It seems inevitable that one of these companies will someday soon propose selling advertising to consumers based on their home energy usage and patterns of usage, the smart-grid equivalent to NebuAd. Imagine an ad that said, "we noticed that you still watch TV on an old cathode-ray tube. Have you thought about upgrading to a flat panel?" When this happens, regulators (the state public utilities commissions) should consider this a significant, deeply worrying privacy lurch, and should consider regulating it under a rule of branded privacy.[332]

This suggestion is consistent with the approach taken by the FTC in its 2012 privacy report.[333] In elaborating the types of "material retroactive changes to privacy representations" that would trigger a requirement of affirmative, express consent, the report gives one concrete example: "at a minimum, sharing consumer information with third parties after committing at the time of collection not to share the data would constitute a material change."[334] This would cover the switch to behavioral advertising discussed above, although it is both broader and narrower.

Regulators should look for recurring scenarios other than behavioral advertising that should qualify as branded privacy triggers. To give only two examples, branded privacy might be tied to decisions to shift private infor-

---

[326] *Id.*

[327] *Id.*

[328] DEP'T ENERGY, 2010 SMART GRID SYSTEM REPORT (2012), *available at* http://energy.gov/oe/downloads/2010-smart-grid-system-report-february-2012.

[329] THE WHITE HOUSE, A POLICY FRAMEWORK FOR THE 21ST CENTURY GRID: ENABLING OUR SECURE ENERGY FUTURE 25–36 (2011), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

[330] *Id.* at 37–48.

[331] Mark Chew, *How to Drive Adoption of a Smart Grid Platform: A Look Inside Trilliant*, MIT ENTREPRENEURSHIP REV. (Sept. 6, 2011, 8:31 PM), http://miter.mit.edu/article/how-drive-adoption-smart-grid-platform-look-inside-trilliant.

[332] For more on the threat to privacy from the smart grid, *see* Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 4–5 (Ctr. for Energy & Envtl. Sec., Working Paper No. 09-001, 2008), available at http://ssrn.com/abstract=1370731.

[333] FTC FINAL REPORT, *supra* note 176, at 57–58.

[334] *Id.* at 58.

mation and behavior to the public sphere (a la Facebook) or to release privately held information to the public (a la AOL in 2008[335]).

2. Migrating Users

Branded privacy can take on a weak or strong form, corresponding roughly to opt-out and opt-in privacy regimes. In the weak form, companies must adopt a new brand name but can migrate all users from the old service to the new service, albeit only after giving notice of the move. The problem with the weak form is the problem with all opt-out regimes: defaults are sticky, and inaction trumps action, meaning users are likely to go along without complaint.[336]

In the strong form of branded privacy, a company cannot migrate users but instead must sign up users by requiring an affirmative action (maybe nothing more than the click of an "I agree" button) to switch. If a company wants to reinvent itself, it can, but only by starting from zero and building user trust in a new brand.

Regulators should probably restrict use of the strong form to contexts where a strong intervention is necessary. Here again are principles rather than precise rules: first, lurches involving sensitive information (such as relating to location, health, education, children, or communications) deserve the strong form. Second, lurches affecting industries with little-to-no true competition should be treated with the strong form of the rule. Third, sectors that are already subject to privacy regulation deserve strong treatment too.

Some might argue that the weak form of branded privacy adds nothing to the regulatory toolkit because it is no different from legacy regulations that mandate notice and opt-out, which many decry as weak.[337] This is a misguided response. Although the weak form of branded privacy bears resemblances to opt-out privacy rules, it is a far stronger form of regulation than opt-out alone.

Weak branded privacy is stronger than unadorned opt-out for at least two reasons, one focused on the inner-workings of the company and the other focused on the external visibility branded privacy provides. First, companies are unlikely to rush into privacy lurches if it causes them to lose their brand, even if they can automatically migrate all of their users. Branded privacy will stimulate much deeper deliberation within a company than opt-out rules can. In fact, companies that have invested a significant amount of time and money in their brand will possibly be more reluctant to move into weak branded privacy than even to an opt-in rule without brand consequences.

Second, the weak form of branded privacy adds significant visibility to the public. Consumers are unlikely to miss the new logo greeting them not only the first time they log in after the switch but for weeks or months afterwards, according to trademark theory.[338] In addition, privacy watchdogs and regulators will find it easier to discuss the switch with one another and with consumers, given the convenient label.

Regardless of whether branded privacy is selected in its strong or weak form, companies should be permitted to continue to use the old brand with users who are not subjected to the new rules. If Facebook wants to create a new service that is much more public than the original, it can create

---

[335] Ohm, *Broken Promises*, *supra* note 93, at 1717–18.

[336] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1256–69 (1998) (discussing "sticky" and "Teflon" default rules for cyberspace privacy).

[337] *See id.*

[338] *Supra* Part II.C.1.

dual versions of the service, giving users the choice between switching to "Facebook World" or staying with "Facebook."

In a similar vein, companies should be allowed to use the old brand for brand new users, users who are not trapped in the information quality problems created during the lurch. Odds are, most companies would not choose this path, enrolling new users under the old name while at the same time showing old users a new name. In most cases, when branded privacy is imposed, companies will switch all users, old and new, to the new name.

3. How Much Must the New Brand Differ?

Any branded privacy solution must specify how much the new brand must differ to comply with the rule. But, once again, regulators should see fit to vary the answer contextually based on the seriousness of the privacy lurch problems they are trying to resolve.

One possibility we should dismiss at the outset is trademark law's "likelihood of confusion" standard.[339] In other words, we should not mandate that the new brand must differ so much from the old brand that consumers no longer will think that the services come from the same source.[340] This would miss the point of branded privacy entirely. The idea of branded privacy is not that the consumer must think (incorrectly) that the new service is produced by a new producer. Rather, the goal is to ensure that the consumer recognizes that the new service is a new thing, from a privacy point of view, helping him try to overcome the information-quality problems he encounters in most online notice-and-choice situations.

How different must two brands be to provide the sufficient amount of differentiation? The standard should be something like, "likely to be noticed." This will turn on the contextual norms, because names probably vary in different ways in different contexts and maybe even in single contexts over time. It is likely that consumer surveys—similar to the ones uses to litigate likelihood of confusion—will be useful, but these surveys should ask different questions.[341]

Given the likely-to-be-noticed standard, it seems that merely increasing a version number should not be enough, at least not without additional empirical proof that consumers pay attention to version numbers. Version numbers are rarely used, at least in any visible way, on the online services focused on most in this Article. Even in the analogous space of software, version numbers seem to mean less today than they once did, due in part to rampant version number inflation.[342]

Allowing version numbers for branded privacy might also invite gaming. If companies can increment version numbers at will whenever they want (to mark some minor change or perhaps with no change whatsoever), they might do so strategically when branded privacy is not in play, to muddy the salience of any particular increment. They might train the consumer, in other words, to disregard version increments, meaning the information-quality benefits of the rule will be lost.

---

[339] Polaroid Corp. v. Polarad Elecs. Corp., 287 F.2d 492 (2d Cir. 1961).

[340] *Id.*

[341] *Cf. id.* (discussing survey evidence used to help establish likelihood of confusion).

[342] Frederic Lardinois, *Browser Version Numbers are Now Irrelevant—And That's a Good Thing*, SILICONFILTER, Aug. 15, 2011 ("[T]here is no good reason why an average user should have to worry about keeping a browser up to date and given the current version number inflation, these numbers have completely lost their meaning anyway.").

Regardless of the precise formulation, the rule should probably allow companies to use their prior marks as a component of the new brand. In other words, companies should be allowed to build what trademark law calls a "family of marks."[343] Brands are extremely valuable things to many companies, particularly those associated with online services.[344] For many companies, the brand may be the most valuable item on the books.[345] Allowing the new brand to be based on the old lessens the burden of branded privacy. This moderates the impact on the market, which likely makes the rule more politically palatable.

Companies facing the branded-privacy rule will probably opt to add a word to its primary brand, think New Coke, Facebook Beacon, or Google Buzz. Ideally, the meaning of the word or words appended will reflect in some way the change that has been made, such as "Facebook World" (for a more public version of the social network service) or "Personal Comcast" (for behavioral-advertising-supported broadband). Whether this is required depends on the goals of the regulator and is not a necessary component of branded privacy. But deceptive marks should never be allowed, meaning we should never see a "Google Private" as a rebrand to describe a new, more invasive service.[346]

4. How Long Should the New Brand Last?

The final variable regulators or legislators might vary is the length of time the company should be required to use the new brand. We might achieve our policy goals without forcing a permanent shift. Companies might be given a time period, say one or two years, during which the new brand must be used (perhaps in conjunction with the old brand). At the end of the period, the rule might be lifted and the old brand restored.[347] The theory is that the negative effect of a privacy lurch fades with time. Privacy lurches disrupt through surprise and by unsettling expectations. After one or two years after a privacy lurch, users—both new and continuing—will have had time to adjust to the new rules and privacy watchdogs and regulators will have had time to have their say.

Sometimes, given the well-documented power of secondary meaning and goodwill accumulation,[348] companies might forego the chance to return to an old name. The company might decide that "Facebook Plus" ends up accumulating so much goodwill that it essentially abandons the bare Facebook name.

---

[343] MCCARTHY, *supra* note 206, at § 23:61 (4th ed. 2012) (discussing the "family of marks rule"). The treatise gives as a well-known family of marks the marks beginning with "Mc" owned by McDonald's Corp. *Id.*

[344] *See* Tim Culpan, *Apple Brand Value at $153 Billion Overtakes Google for Top Spot*, BLOOMBERG (May 8, 2011), http://www.bloomberg.com/news/2011-05-09/apple-brand-value-at-153-billion-overtakes-google-for-top-spot.html (stating Apple's brand value at $153.3 billion and Google's brand value at $111.5 billion).

[345] *Id.*

[346] *Cf.* MCCARTHY, *supra* note 206, at § 11:54 (discussing "deceptive and deceptively misdescriptive marks").

[347] *Cf.* Note, *Badwill*, 116 HARV. L. REV. 1845, 1862–63 (2003) (suggesting that firms seeking to change a product's brand name to escape an accumulated negative reputation—or badwill—be given a period of time during which they must continue to use the old name).

[348] Landes and Posner, *supra* note 192, at 270.

## C. Implementation

Branded privacy can be implemented in law in at least three different ways. First, competitors or aggrieved parties might argue in trademark litigation that a company abandoned its mark when it shifted its privacy policies, although this theory is likely to be rejected. Second, the Federal Trade Commission might argue that dramatic shifts in a company's core privacy commitments represent an unfair and deceptive trade practice unless carried under a new name. Third, Congress or state governments can consider enacting new consumer protection or trademark laws to implement branded privacy.

### 1. False Advertising Law

Branded privacy might result from lawsuits brought under false advertising causes of action. For example, competitors who "believes that he or she is likely to be damaged" by the change in the service, might sue under section 43(a)(1)(B) of the Lanham Act, which prohibits "misrepresent[ing] the nature, characteristics, qualities, or geographic origin" of goods or services.[349] The essence of this cause of action is the deception on the consumer.

Section 43(a) has been applied to what Shahar Dillbary calls the "intra-brand setting," meaning to cases in which trademark owners have been found to deceptively change the qualities of the underlying product.[350] Thus, courts have applied false advertising to the use of the mark "Polysapphire" to products lacking sapphires;[351] "Gelatin Snacks" without any gelatin;[352] and "Ricelyte" to a rice-less product.[353]

There is an important difference between branded privacy and these cases—these precedents each involve a descriptive mark. The deception resides in the direct communicative message the name itself provides: this contains sapphires; this contains rice.[354] Branded privacy requires an additional step: the reason the use of the mark Facebook is after the most recent switch is because consumers have learned to associate the name with an inherently-private service.

The problem, as Dillbary discusses in depth, is that courts have refused to extend section 43(a) to cases involving trademarks that are not descriptive.[355] He traces the reluctance to apply section 43(a) in such cases to *Alfred Dunhill, Ltd. v. Interstate Cigar Co.*, another rebuilt product case.[356] In *Dunhill*, the Second Circuit held that false advertising law did not apply to the potentially deceptive messages communicated through a non-descriptive mark.[357] "Not every possible evil has yet been proscribed by federal law."[358] This case, and its progeny, are likely a unyielding stumbling block to false advertising cases premised on privacy lurches.[359]

---

[349] 15 U.S.C. § 1125(a)(1)(B).
[350] Dillbary, *supra* note 292, at 355.
[351] Johnson & Johnson v. GAC Int'l, Inc., 862 F.2d 975 (2d Cir. 1988).
[352] Kraft Gen. Foods, Inc. v. Del Monte Corp., 28 U.S.P.Q.2d 1457 (S.D.N.Y. 1993).
[353] Abbott Labs v. Mead Johnson & Co, 971 F.2d 6, 14 (7th Cir. 1992).
[354] Dillbary, *supra* note 292.
[355] *Id.*
[356] 499 F.2d 232 (2d Cir. 1974).
[357] *Id.* at 235-36.
[358] *Id.*
[359] False advertising might apply to a good or service whose very name describes a privacy promise, such as the web proxies called Privoxy, http://www.privoxy.org, and Anonymizer, http://www.anonymizer.com. But none of the examples given in Part I involve this kind of name.

2. Trademark Abandonment

According to McCarthy, "Since a trademark is not only a symbol of origin, but a symbol of a level of quality, a substantial change in the nature or quality of the goods sold under a mark may so change the nature of the thing symbolized that the mark becomes fraudulent or that the original rights are abandoned."[360] Plaintiffs might try to rely on this kind of reasoning to convince courts to implement branded privacy in trademark litigation. Civil litigants might claim, for example, that Facebook abandoned its mark when it switched from being a private to a public service. This theory faces several significant, and probably insurmountable, hurdles.

This form of abandonment has rarely been found. The McCarthy treatise cites only one example, a 1910 case in which the manufacturer of SOLAR alum baking powder forfeited trademark rights by selling the mark to another who substituted phosphate for alum.[361] Courts are unlikely to apply this rule in privacy lurch cases, perhaps by holding that a shift in privacy, although important, constitutes a minor variation not a wholesale change.[362]

Perhaps even more devastatingly, the branded-privacy-by-trademark-litigation theory runs aground on the unfavorable mechanics of trademark litigation.[363] Courts have held that consumers do not have standing to sue under the Lanham Act.[364] Instead, the consumer protection goals of trademark law are advanced through competitors using similar marks, the only parties given standing to accuse a company of infringing a trademark. In most privacy-lurch situations, no such competitor will exist. For similar reasons, administrative filings at the USPTO to oppose registration or to request cancellation of a mark are also unlikely to be a useful vehicle for branded privacy.[365]

3. FTC Power to Police Unfair and Deceptive Trade Practices

The FTC might use its section five power to police "unfair or deceptive acts or practices" to link a brand to a particular level of privacy.[366] This might be the best way to implement branded privacy because it likely represents a new remedy for the FTC but not a new substantive rule. As summarized in the recent FTC privacy report, "[u]nder well-settled FTC case law and policy, companies must provide prominent disclosures and obtain opt-in consent before using consumer data in a materially different manner than claimed when the data was collected, posted, or otherwise obtained."[367]

Thus, in 2004, the FTC investigated alleged privacy violations by the owners of a website used to sell products sold under the "Hooked on Phonics"

---

[360] MCCARTHY, *supra* note 206, at § 17:24.

[361] *Id.* (citing Indep. Baking Powder Co. v. Boorman, 175 F. 448 (C.C.D.N.J. 1910)).

[362] *See, e.g.,* Marlyn Nutraceuticals, Inc. v. Mucos Pharma GmbH & Co., 571 F.3d 873 (9th Cir. 2009) ("Trademark owners are permitted to make small changes to their products without abandoning their marks.").

[363] Perzanowski argued that trademark law was not a useful vehicle for protecting consumers from harmful corporate "unbranding," such as Blackwater's decision to rebrand itself Xe, because of "structural limitations" of trademark law, namely the fact that "[c]onfusing uses of a firm's own marks are largely unregulated by trademark doctrine." Perzanowski, *supra* note 295, at 27.

[364] *E.g.* Colligan v. Activities Club of New York, Ltd., 442 F.2d 686 (2d Cir. 1971); Dovenmuehle v. Gilldorn Mortg. Midwest Corp., 871 F.2d 697 (7th Cir. 1989); Serbin v. Ziebart Int'l Corp., 11 F.3d 1163 (3d Cir. 1993); Barrus v. Sylvania, 55 F.3d 468 (9th Cir. 1995).

[365] MCCARTHY, *supra* note 206, §§ 20:7, 20:46.

[366] 15 U.S.C. § 45(a)(1) (2006).

[367] FTC PRIVACY REPORT, *supra* note 151, at 77.

brand name.[368] The complaint alleged that the company, Gateway Learning, made promises in privacy policies dating back to 2000 that it did "not sell, rent or loan any personally identifiable information regarding our consumers with any third party unless we receive a customer's explicit consent."[369] Contravening this promise, the company began "renting" personal information, "including first and last name, address, phone number, and purchase history," without first obtaining consent.[370] The company settled the case with the FTC after entering into a consent agreement that required opt-in consent for sharing data with third parties.[371]

Of even closer applicability, in 2011, the FTC accused Facebook of "deceiv[ing] consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[372] Among the many charges filed in the complaint, the FTC specifically faulted Facebook because, "In December 2009, Facebook changed its website so certain information that users may have designated as private—such as their Friends List—was made public. They didn't warn users that this change was coming, or get their approval in advance."[373]

Although privacy watchdogs generally lauded the settlement, some argued that it highlighted the somewhat toothless powers given to the agency.[374] The FTC lacks the ability to levy fines against companies for unfair and deceptive trade practices. And sometimes the agency lacks will, not power. For example, in the Facebook settlement, it declined to order Facebook to roll back the "default public" settings it had thrust on millions of its users without their consent.

The Facebook settlement would have been an excellent test case for branded privacy. Nothing seems to prohibit the FTC from treating a trademark itself as a component of a company's disclosure, one that can later be part of a remedy for unfair or deceptive trade practices.[375] Going forward, companies should know that the agency is willing to treat violations in this way. Companies that cause significant, harmful privacy lurches like Facebook's should pay the price with a new name. Perhaps even more importantly, the threat of branded privacy should play a notice-forcing rule, by convincing companies to elaborate their core privacy commitments clearly and unambiguously at their launch.

Finally, even if the FTC chooses not to so aggressively assert power over a company's trademarks, it might seek to extract changes to trademarks as an important condition in consent agreements.

4. New Legislation

Although the FTC might be able to implement this change, in case there is doubt about the agency's ability and willingness to do so, Congress

---

[368] *In re* Gateway Learning Corp., 138 F.T.C. 443 (2004).
[369] *Id.*
[370] *Id.*
[371] *Id.*
[372] Fed. Trade Comm'n, Press Release: Facebook Settles FTC Charges That it Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm.
[373] *Id.*
[374] Grant Gross, *Privacy Groups Generally Cheer FTC's Facebook Settlement*, PCWORLD.COM, Nov. 29, 2011, http://www.pcworld.com/businesscenter/article/245162/privacy_groups_generally_cheer_ftcs_facebook_settlement.html.
[375] Perzanowski, *supra* note 295.

and state legislatures might consider implementing the change statutorily instead. Given the pre-existing dual federal-state framework for legislating trademarks and unfair competition, even a State legislature wields substantial power in this space.[376]

Congress might consider, for example, a new law that obligates a company possessing information about users to associate its registered federal trademarks to a core set of privacy promises. The legislation could even specify a standardized format for this disclosure, bolstering the notice-forcing function of branded privacy. When changes are made to these core policies, the law should provide at least concrete FTC jurisdiction to order the use of a new trademark. If Congress wants to spur even more enforcement activity, it could offer individual aggrieved consumers a cause of action to pursue this remedy as well. It probably would not be wise to provide damages in these cases, but an injunctive remedy and the opportunity for cost and fee reimbursement would probably do much to bolster the effect of the law.

In fact, Congress has been provided an excellent immediate opportunity for this change, as the White House has recently exhorted it to enact a new comprehensive baseline privacy law implementing its Consumer Privacy Bill of Rights.[377]

Putting the prescription together, Congress could enact a new law modeled on the following:

> (A) ENHANCED NOTICE OF MATERIAL CHANGES TO PRIVACY POLICIES. No entity possessing personal information about any individual shall make a material change to information-handling policies and procedures without giving notice to its users by assigning a new name to its affected products or services.
>
> (B) DEFINITION. As used in this Part—
> (1) "material change to information-handling policies" means any change that materially affects the risk of significant privacy harm to any individuals and should be further defined by the FTC as provided below.
>
> (C) FTC ENFORCEMENT. The Federal Trade Commission is empowered to enforce the provisions of this section and must promulgate regulations within eighteen months implementing this section.
>
> (D) PRIVATE ENFORCEMENT. Any person aggrieved by a material change to information-handling policies may bring civil suit to enforce this section with remedies limited to:
> (1) an injunction ordering the use of a new trademark or service mark;
> (2) costs; and
> (3) fees.

[376] *But see* WHITE HOUSE WHITE PAPER, *supra* note 151, at 37–38 (calling for a new federal statute for consumer privacy that "preempt[s] State laws to the extend they are inconsistent" with it).
[377] *Id.* at 35–36.

## D. Examples

### 1. Revisiting the Four Examples

Let us revisit the four privacy lurches from Part I to see how branded privacy might have been applied in response to each. The simplest example is the rise of NebuAd and Phorm.[378] These companies tried to supply broadband cable Internet services with systems that would watch their user's web-surfing habits in order to build profiles that could be sold to advertisers.[379] These new services represented a significant privacy lurch. In many cases, they would have cut against express promises made by the cable companies in prior privacy policies, which prompted some companies to send letters to affected customers alerting them to the change.[380]

Under any form of branded privacy, broadband internet companies would not be allowed to embrace NebuAd's or Phorm's new business models using their old brand names, even with user consent. Broadband companies have *never* monitored users in this way or to this extent.[381] In fact, given the heavy regulation of the telecommunications industry, this activity was probably already illegal without express consent. For one thing, the FCC's so-called "CPNI" regulations might prohibit it.[382] And the federal Wiretap Act arguably makes it a felony for companies to engage in this kind of surveillance.[383]

A regime of branded privacy would not prevent companies like Charter from partnering with companies like NebuAd, but it would require Charter to launch such a service under a new name, say "Charter Personal" or "Tailored Charter." Perhaps Charter would offer this to customers in competition with plain ordinary "Charter" service, using price as a way to differentiate the products.

The cell-phone-location scenario leads to almost identical results. Companies like Verizon Wireless or AT&T Wireless might someday decide that the rich databases they maintain containing location information are a treasure trove for marketers.[384] They might sell access to this database, for example, to advertisers who want to direct ads to people who have visited a particular mall, amusement park, or hospital. Obviously, a person's physical location is extremely sensitive information and the risk to personal privacy (if not physical safety) is plain.[385]

Cell phone providers that began to sell customer location information would be cutting back on decades of privacy promises. And, just like the broadband Internet companies, cell phone providers have been heavily regulated for decades. In fact, they are subject to precisely the same CPNI and

---

[378] *Supra* Part I.B.2.

[379] Ohm, *Rise and Fall, supra* note 51.

[380] Hansell, *supra* note 174.

[381] Ohm, *Rise and Fall, supra* note 51.

[382] Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, *Report & Order & Further Notice of Proposed Rule Making*, 22 FCC Rcd. 6927 (2007), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf.

[383] 18 U.S.C. § 2511(1)(a); Ohm, *Rise and Fall, supra* note 51.

[384] *See* Simonite, *supra* note 75.

[385] In fact, location information is so sensitive, there is a good argument it should be regulated outright, and Congress is currently considering several bills which would do so. *Supra* note 72. This section focuses primarily on the problem of the privacy lurch, but a prohibition on marketing based on location would of course take precedent.

Wiretap rules discussed above, both of which might cover location information.[386] For these reasons, Verizon would need to launch "Verizon Personal" and AT&T would need to launch "AT&T Personal" to justify such a shift.

In fact, both of these examples suggest the need for the "strong" form of the brand privacy solution, which requires not only a new name, but also prevents an automatic migration of users. Both of these models demand opt-in not opt-out treatment. Given the long track record of respectful privacy practices, the sensitivity of the information, and the history of close regulation, Verizon, AT&T and Charter should be required to convince customers to switch to their new, rebranded "Personal" versions rather than be permitted to migrate customers without consent.

We move now to two companies that have not historically been subjected to much privacy regulation: Facebook and Google. Would Facebook's slow lurch from being strictly private to mostly public have triggered branded privacy?[387] It is fair to say that Facebook is fundamentally a different service today than at the time of its launch in 2004, from a privacy point of view. This evolution can be traced contractually through the many versions of its privacy policy.[388]

Under the rules of branded privacy, Facebook would have needed to re-launch at some point as "Facebook World" or "Facebook Public," albeit only for a limited time, perhaps a year or two. This fairly easy case raises two minor complications. First, because Facebook evolved slowly to its public state, regulators might have found it difficult to isolate the precise moment when it needed to order the use of a new brand. This is far from being an exact science, however, and even if a regulator cannot tell whether any particular single step taken by Facebook justified the requirement for a new name, it can be sure that when one compares the present form of Facebook with its 2005 practices, the moment at which Facebook fell under the burden of branded privacy passed long ago.

Second, Facebook should not have been able to avoid its rebranding fate by pointing to the fact that it provided privacy settings its users could toggle to use Facebook in a less-public way. Privacy settings are notoriously difficult to use, and researchers have shown that users struggle with Facebook's labyrinthine settings in particular.[389] Even though users can opt into better privacy than the default, many will not, so the default setting is what regulators should assess. In this case, the new default setting would have triggered a new brand requirement.[390]

Finally, this brings us to Google's March 2012 move tearing down walls separating databases collected from different services. Even though this act represented a significant and undeniable privacy lurch, Google might not have been forced under the rules prescribed above to adopt a new name. This is because even though the March shift apparently shifted Google's practices

---

[386] *Supra* notes 382–383.

[387] *Supra* Part I.B.4.

[388] *Id.*

[389] Michelle Madjeski, Maritza Johnson, & Steven M. Bellovin, *The Failure of Online Social Network Privacy Settings* (2011), https://mice.cs.columbia.edu/getTechreport.php?techreportID=1459.

[390] In Facebook's case, some of the "default public" choices cannot be turned off with privacy settings. Opsahl, *supra* note 78 ("Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings.").

significantly, it may not have contravened any specific policies, shedding light on the muddled information quality of corporate pronouncements about privacy and starkly demonstrating why branded privacy must work hand-in-hand with new pressure for notice forcing.

At least as far back as 2005, Google's privacy policy explained that "[w]e may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services. For certain services, we may give you the opportunity to opt out of combining such information."[391] But based upon the events of the past few months, it appears that the company's practices were out of sync with their policies. Can a pattern of practice give rise to a privacy commitment that triggers branded privacy, even if express privacy policies allow different behaviors? In other words, can actions trump contracts for purposes of this rule?

If a company explicitly and publicly promises—through marketing or comments to regulators—more privacy than the floor set in their contracts, this should give rise to a branded privacy commitment.[392] Because branded privacy is about commitments (and in the case of FTC enforcement, unfair and deceptive trade practices[393]) and not binding contracts, it need not be limited to the words within the four corners of the contract alone.

But even with this gloss, the branded privacy case against Google is unclear. Although the 2005 privacy policy excerpted above alerts consumers to the possibility that data might be combined, we would need to review all of the "more than 70" privacy policies that also existed at the time.[394] Did the contracts for YouTube and Google Docs and Google Calendar also provide the same notices?

It is thus unclear whether the FTC or a plaintiff lawsuit could have forced Google to rebrand due to the March 2012 switch. This speaks once again to the need to couple branded privacy with some sort of notice-forcing mechanism, be it a new rule, a piece of legislation, or merely the incentive that comes from the stated intention by a regulator to enforce a powerful new rule. The fact that Google's privacy commitments before this switch were shrouded in a mix of privacy policies, practices, and public statements highlights why branded privacy plus notice-forcing rules are so needed. Once we implement branded privacy, companies that try to release confusing signals about their true designs will stand out from the crowd by their behavior.

2. Examples of Branded Privacy from the Past

If branded privacy had been the rule, a company like Google might have embraced the idea of selecting a new name voluntarily. Google could have declared that for one year, their newly combined services would bear a logo saying "New Google," as part of a wide-ranging campaign for public notice. Doing this unilaterally would have signaled to both the public and

---

391 Google's Privacy Policy, GOOGLE, http://www.google.com/policies/privacy/archive/20051014/ (last visited Mar. 27, 2012).

392 *Cf.* Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635 (2011) (urging courts to take into consider software design when interpreting online contracts).

393 Susan Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 2 (2009) (noting that FTC section five actions turn not on contract principles but instead on whether acts are unfair and deceptive).

394 Whitten, *supra* note 37.

regulators that the company intended to go well beyond what the law required in an effort to put every single customer on notice.

Consider how often companies have relied voluntarily upon something like branded privacy in the past. Many companies have launched new, privacy-invasive services under distinct brand names, implicitly understanding the way a new brand can alert people to change. They have done this not because a law or regulator has asked them to do it, but because their own internal business incentives suggested they do so.

When Facebook launched its controversial social marketing platform, it called it Beacon.[395] When the company changed user profiles to make it easier for users to access old data—and most notably old photos—of other users, it called the feature Timeline.[396] In each case, the company implemented the new feature as an "opt-out" feature, meaning all users were forced to use it by default.[397] Whether this use of the weak form of branded privacy is sufficiently privacy-protective is not clear, but the fact that the company has associated so many new names with their service shows the power of the rule.

Google has also embraced the strategy, for example, in launching "Buzz" and "Google Plus," its two highest-profile forays into providing social networks.[398] Google also launched its email platform under an entirely new name, "Gmail." Gmail is a fascinating case study, because it shows how a new name can focus the mind of the consuming public about incipient privacy risks. And it also serves as a reminder of the limits of privacy law, because sometimes the consuming public, faced with truthful full disclosure about a service's privacy choices, will nevertheless choose the bad option for privacy, at which point there is often little left for privacy advocates and regulators to do.

At the initial launch of Gmail, Google weathered a storm of fierce criticism because the service featured contextual advertising.[399] Ads appear alongside a user's inbox, tailored to the content of the message being displayed. Privacy activists decried the way Google seemed to be breaching the well-developed norms of email, offering a service that complicated the previously bright lines between public and private.[400] Some called for a boycott or a government investigation.[401]

But the storm of criticism did not stick. Users signed up for Gmail accounts by the millions,[402] and criticisms of its contextual advertising seem

---

[395] McGeveran, *supra* note 12.

[396] Facebook, *Tell Your Story with Timeline*, THE FACEBOOK BLOG (Sept. 22, 2011), http://www.facebook.com/blog/blog.php?post=10150289612087131.

[397] Timeline is opt-out only in a rough sense of the word. Users are forced to use it, but diligent users can mark old posts individually to cause them not to appear in their Timeline. Jill Duffy, *12 Things You Should Know About Facebook Timeline*, PC MAG.COM (Jan. 25, 2012), http://www.pcmag.com/article2/0,2817,2393464,00.asp.

[398] *Introducing the Google+ Project: Real-Life Sharing, Rethought for the Web*, GOOGLE OFFICIAL BLOG (June 28, 2011, 11:45 AM), http://googleblog.blogspot.com/2011/06/introducing-google-project-real-life.html; *Introducing Google Buzz*, GOOGLE OFFICIAL BLOG (Feb. 9, 2010, 12:06 PM), http://googleblog.blogspot.com/2010/02/introducing-google-buzz.html.

[399] Chris Gaither, *Google's E-Mail Strategy Criticized*, L.A. TIMES, April 2, 2004, at C1.

[400] *Id.*

[401] Electronic Privacy Information Center, *Gmail Privacy FAQ*, http://epic.org/privacy/gmail/faq.html (urging for a boycott and discussing state legislative proposals) (last visited March 29, 2012).

[402] Erick Schonfeld, *Gmail Grew 43 Percent Last Year. AOL Mail and Hotmail Need to Start Worrying*, TECHCRUNCH, Jan. 14, 2009, http://techcrunch.com/2009/01/14/gmail-

today to have faded. The lesson product designers should draw from Gmail is not that contextual advertising of the inbox is not unusually violative of privacy. The better lesson is that you never have a second chance to make a first impression. Gmail set (mostly) transparent privacy rules from birth. Before its developers began enrolling the masses, they made it well-known that they were changing the status quo.

Although some critics continue to point to Gmail as an example of how ordinary consumers can sometimes fail to understand the way new services risk individual privacy, I am not sure I agree. In the landscape of the privacy risks to which consumers have been subjected, I am much less troubled by Gmail than I am by Google's March 2012 database consolidation in part because the new name and opt-in design of Gmail leaves me confident that most Gmail users joined the service at least aware of the privacy risks.

## E. Potential Critiques and Responses

Some might object that branded privacy unnecessarily intrudes on a free market. On the contrary, this solution seems much more deferential to the market than other proposals that have been advanced. For example, some proposals urge a much more sweeping reworking of contract law, one that might call into question even minor or unimportant terms in privacy policies or even online contracts with consumers outside the privacy context.[403] My proposal instead restricts itself to a few unusually important forms of privacy promises, those worthy of being part of branded privacy's trigger list, with no effect on promises that go beyond that list.

This proposal is also more deferential to the market than proposals that would restrict or severely limit what holders of data are allowed to do with user information. Under branded privacy, services can be born non-private, and when they are, they can remain that way, assuming their creators exercise meaningful notice and consent and take steps to prevent harmful downstream uses. Twitter, which unlike Facebook was born inherently public, can continue to use its brand without limit.

Another market-focused objection might center on how the proposal might harm innovation by preventing start-up companies from experimenting with new privacy settings. This brings us back to where we started,[404] to the dynamic benefits of pivots.[405]

This is a serious objection, but one that can be easily addressed. Any implementation of the rule should include a "first milestone rule," one that forestalls application of the rule until a predefined moment in the lifecycle of a service. The first milestone might be a certain number of users, say 10,000.[406] Until a service reaches 10,000, the terms of branded privacy are not yet set. Or the milestone might be defined with a less rigid standard such as the moment when the service goes beyond "friends and family" or when

---

grew-43-percent-last-year-aol-mail-and-hotmail-need-to-start-worrying/ (estimating Gmail having nearly thirty million users).

[403] Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635 (2011); Andrea Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529, 560–61 (2007).

[404] *Supra*, Part I.A.

[405] Jenna Wortham, *In Tech, Starting Up by Failing*, N.Y. TIMES, Jan. 17, 2012, at B1.

[406] In the final draft of the FTC Privacy Report, released March 26, 2012, the Commission exempted any company collecting "non-sensitive data from fewer than 5,000 consumers a year" in order "to address concerns about undue burdens on small businesses." FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

the service begins taking registrations from the general public. Other possibilities might tie the first milestone to venture capital funding, an IPO, or even the "alpha/beta/release" labels that websites already use.

Another objection builds on themes raised in both of the first two objections: the plan might unfairly privilege start-up ventures over incumbent players. Because the rule is triggered by change to initial promises, only incumbent players are saddled by its requirements meaning the proposal disrupts the ordinarily evolution of a market. This objection is the easiest to rebut, for nothing in the proposal prevents an incumbent from entering into a market with a privacy-invasive business model. The rule simply requires the incumbent to give up its old brand (and maybe its old roster of users) in order to compete in the new space.

In fact, the rule might produce the happy side-effect of *increasing* competition. Incumbents will no longer be able to create successful services based primarily on their favorable market share and the inattentiveness of their customers. The rule will place a thumb on the side of the scale of the upstart new entrant, but not as a matter of competition policy. Instead, this approach reflects what economics and psychology and computer science suggest as a better way to overcome fundamental information-quality problems during times of change. The resulting framework triggers meaningful notice and consent and is thus likelier to lead to consumer privacy. And lest we feel too badly for incumbents, we should remember the many other structural advantages incumbents enjoy, from well-honed efficient processes, to political power, to ready access to vast amounts of capital. From among a long list of benefits the incumbent enjoys, we are removing only one, exclusive control over a brand.

Strong privacy advocates—those who embrace rights-based FIPPs—will lodge the kind of complaints they lodge against all notice-and-choice regimes. First, because branded privacy gives companies the option of selecting zero privacy, it does too little to protect users from predatory companies. To this, I must emphasize that branded privacy is meant as one solution targeting the special problem of the privacy lurch, but it is not meant to preempt other solutions focused on other contexts. Proposals to regulate much more aggressively and thoroughly certain sectors that tend to traffic in highly sensitive information, for example, should be pursued and would be complementary, not contradictory, with rules mandating branded privacy.

Another complaint we might hear from privacy advocates is that users will become desensitized to this form of notice and choice over time.[407] I doubt this is the case, because trademark theory teaches us about the information-signaling power of a logo or trademark. In addition, because mandated rebranding will occur only for significant privacy shifts and given the amount of accumulated capital most companies hold in their brands, rebranding will probably be a very rare event, one that privacy advocates themselves will be well-equipped to bring to the attention of consumers who might not notice the change themselves. The point of branded privacy is not to spawn a crazily shifting landscape with brand names of prominent services changing weekly. Instead, and perhaps somewhat ironically, branded privacy will probably result in stability, because it will force companies to engage in much more initial internal deliberation about what type of privacy strategy they want to embrace—enabling Privacy by Design—and it will force them to

[407] *Cf.* Grimmelmann, *Product Safety*, *supra* note 16, at 812 ("Demanding explicit consent every time information is shared with someone other than its specific, original audience could require hundreds of prompts, per user, per day.").

abandon deceptive bait-and-switch strategies that today seem far too appealing.

Others might respond that the proposal unnecessarily duplicates the role of certification marks. The Lanham Act and many state trademark laws allow the protection of marks that "certify" some quality of an underlying good or service, with some certifying authority taking on the responsibility of policing quality.[408] For privacy, several organizations have introduced privacy certification authorities, most notably TRUSTe and BBBOnline.[409] Without delving too deeply into ongoing debates about the efficacy and importance of self-regulatory privacy efforts,[410] it is enough to say that certification marks do not have a exemplary track record. TRUSTe, by far the most prominent of the efforts, switched from a non-profit to a for-profit model in 2008, and today collects hundreds of thousands of dollars from some certified entities,[411] which casts a shadow on its claims of impartiality.

More to the point, neither TRUSTe nor BBBOnline extend the kind of sweeping scrutiny of changes made to privacy policies proposed in this Article. And, most fundamentally, a certification logo buried at the bottom of a smartphone screen is a far less powerful symbol of privacy policy details than a rebranded logo sitting in a place of prominence.

Finally, some might wonder why rebranding should be limited merely to privacy policies. Should companies be forced to choose new brand names whenever they alter any important policies such as product safety, environmental practices, political contributions, worker treatment, and relationships with totalitarian regimes? In some ways, this echoes Douglas Kysar's rebuttal to what he calls the product/process distinction, the idea that consumers and regulators should legitimately focus only on information relating to a product (such as consumer safety or privacy) and not to information relating to the processes that lead to the product (such as treatment of workers), an idea Kysar strongly opposes.[412]

I offer two responses, one pushing back mildly on Kysar's argument, or at least arguing that it does not apply to this situation, but the second embracing Kysar's point wholeheartedly. Pushing back, it is easier to justify tying a trademark to policy changes about privacy than it would be to other types of changes. First, as demonstrated repeatedly throughout this article, the regulation of online privacy has centered entirely on notice and choice, and this regulatory history is less well-developed in other areas. The rich body of scholarship challenging privacy policies have focused almost entirely on privacy-specific terms, and less work has been focusing on terms in other online contracts. Second, the privacy policies of a company are tied much more directly than other "process-based" decisions of a company. For an

---

[408] See 15 U.S.C. § 1054 (2006) (permitting registration of collective and certification marks); id. § 1127 (defining collective and certification marks).

[409] *See* Xinguang Sheng & Lorrie Faith Cranor, *An Evaluation of the Effect of U.S. Financial Privacy Legislation Through the Analysis of Privacy Policies*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 943 (2006).

[410] *See*, *e.g.*, Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J. L. & Pol'y for Info. Soc'y 355 (2011); Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation*, 34 SEATTLE U.L. REV. 439 (2011).

[411] Claire Cain Miller, *A Badge That Tells Customers, 'Trust This App'*, N.Y. TIMES BITS BLOG, Sept. 27, 2010, http://bits.blogs.nytimes.com/2010/09/27/a-badge-that-tells-consumers-trust-this-app/.

[412] Douglas A. Kysar, *Preferences for Processes: The Process/Product Distinction and the Regulation of Consumer Choice*, 118 HARV. L. REV. 526, 530 (2004).

Internet service, levels of privacy often go to the essence of what the service offers.

But, in truth, I do not think I have identified a unique bond between brand names and privacy policies. Instead, I am open to the idea that I have identified a new tool that can be placed in many different regulatory toolboxes beyond privacy. Trademarks are supposed to symbolize stability and quality, and companies too often defeat that goal through strategic reinvention. When these fits of reinvention lead to significant risk of harm—as they do during a privacy lurch—it makes sense to consider putting rebranding remedies on the table.

## CONCLUSION

Dynamism sometimes comes at a cost. Companies embrace new business models in order to keep up with competitors and a rapidly evolving technological landscape. But sometimes they do it riding on the backs of their customers, converting databases full of personal information into profits, particularly by shifting to new advertising-based models. This disrupts the expectations of users and contradicts claims of meaningful notice and choice.

This Article has presented an aggressive but still middle-way proposal: tie a company's initial privacy practices to its trademark. Better than a ban on sudden shifts, this remedy leaves freedom for corporate reinvention and also addresses the information-quality problems that have plagued earlier proposals based on notice. Better than a do-nothing embrace of market deference, it envisions an active and important role for government regulators, and it has the teeth necessary to check some of the natural excesses the market ordinarily incentivizes.

The benefits are many: companies will think more about privacy at the outset, choose business models that sacrifice user privacy more deliberatively and at an earlier stage, announce their decisions publicly and unambiguously, and think twice before breaking their promises. Consumers will learn to rely more on company promises, notice significant changes much more frequently, and less often find themselves baited by a good service planning for the day it will become bad. Finally, privacy advocates and government regulators will have a powerful new tool in their arsenal to combat a commonly recurring and important information privacy problem.