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.” [FN4] 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. [FN5] 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. [FN6] Over the past few years, Facebook has incrementally shifted its default settings from providing robust privacy to allowing public scrutiny of its users' personal information. [FN7]

Privacy lurches like these disrupt long-settled expectations. They foist new ground rules upon millions of users whose attention spans have long since waned. [FN8] 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.*910 [FN9] 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 specific 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). [FN10]

But despite the many problems with privacy lurches, some might argue we should do nothing to limit them. Privacy lurches are products of a dynamic marketplace for online goods and services. [FN11] 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. [FN12] 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 lurch-
es, 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. [FN13] 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, *911* written by sophisticated parties with an incentive to hide the worst parts. [FN14]

To breathe a little life back into notice-and-choice, this Article looks to brands and trademarks, representing a novel integration of two very important but until now rarely connected areas of information policy. [FN15] Trademark laws recognize how certain words and symbols in the marketplace tackle the very same information quality and consumer protection concerns that animate notice-and-choice debates in privacy law. Scholars who study marketing, branding, and trademark theory describe the unique informational power of trademarks, service marks, and, more generally, brands to signal quality and goodwill to consumers concisely and unambiguously. [FN16] 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. [FN17]

This Article proposes that we use the 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 *912* name to a fully specified set of core privacy commitments. [FN18] 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 trademark law. It builds on the work of privacy scholars who have looked to consumer protection law for guidance. [FN19] Just as companies selling inherently dangerous products are obligated to attach warning labels, [FN20] so too should companies shifting privacy practices in inherently dangerous, expectation-defeating ways be required to warn their customers. [FN21] And the spot at the top of every Internet web page displaying the brand name may be the best available space 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 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 never before been identified as a separate scholarly “movement,” and whom I am giving the moniker “the New Trademark” scholars--who reconceptualize trademarks as swords used on behalf of consumers rather than merely as shields used to defend producers. [FN22]
At the same time, this solution strikes a balance between the positive aspects of dynamism and the negative harms of privacy lurches. It leaves room for market actors to innovate by focusing 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. Companies will be free to evolve and 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 consider the class of choices consumers care about most, without preventing dynamism 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.

* * *

III. BRANDING PRIVACY

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. [FN226] 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. [FN227] 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 many theories that have been advanced by scholars of both information privacy and trademark law. Consider the teachings of each field in turn.

*945 1. Branded Privacy and Privacy Law Theory

Branded privacy sits comfortably within theories of information privacy law in at least four 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,” [FN228] 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.

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. [FN240] Building on the work of others, he develops parallels between privacy and product safety, expanding familiar tort principles to online privacy problems. [FN241]

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. [FN242] “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.” [FN243] *949 This seems especially important to alert users to unexpected change. [FN244]

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 can subject 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.” [FN245]

In product safety, warning labels must be placed in conspicuous places, likely to be seen just at the moment the risky behavior commences. [FN246] 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 website? 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. [FN247] Courts construing online contracts have gone further, parsing a website into different parts, some more conspicuous than others. In Specht v. Netscape Communications Corp., the 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. [FN248] The FTC’s report entitled Dot Com Disclosures provides similar advice. [FN249]

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 *950 (NAI) voluntarily agreed to place explanatory icons directly on targeted ads
to warn consumers about the targeting being used. [FN250]

But most other online interactions lack such an obvious location 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. [FN251] 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, 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 means that more 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. [FN252] Large, conspicuous warning labels are not compatible with this medium. [FN253]

*951 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. [FN254]

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, considering this aspect of branded privacy “a feature, not a bug.” [FN255] 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. [FN256] Many have complained that there is no market for privacy. [FN257] I think part of the problem*952 is the murky market 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. [FN258] 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.