Branding Privacy

Paul Ohm
Associate Professor, University of Colorado School of Law
paul.ohm@colorado.edu | http://paulohm.com

Forthcoming 97 MINNESOTA LAW REVIEW ___ (2013)

This Article focuses on the problem of what some have called the "privacy lurch," which I define 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 about users 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 adequate notice and choice. They expose users to much more risk to their individual privacy than the users might have anticipated or desired, assuming they are paying attention at all. Given the special and significant problems associated with privacy lurches, this Article calls on regulators to seek creative solutions to address them.

But even though privacy lurches lead to significant risks of harm, some might argue we should do nothing to limit them. Privacy lurches are the product of a dynamic marketplace for online goods and services. What I call a lurch, the media instead tends to mythologize as a "pivot," a welcome shift in a company's business model, celebrated as an example of the nimble dynamism of entrepreneurs that has become a hallmark of our information economy. Before we intervene to tamp down the harms of privacy lurches, we need to consider what we might give up in return.

Weighing the advantages of the dynamic marketplace against the harms of privacy lurches, this Article prescribes a new form of mandatory notice and choice. To breathe a little life into the usually denigrated options of notice and choice this Article looks to the scholarship of trademark law, representing an integration of two very important but too-rarely connected areas of information law. This bridge deserves to be built, as the theory of trademark law centers on the very same information quality and consumer protection concerns that animate notice and choice debates in privacy law. These theories describe the important informational power of trademarks (and service marks and, more generally, brands) to signal quality and goodwill to consumers concisely and efficiently. Trademark scholars also 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. In short, the information qualities of trademarks can meet the notice deficiencies of privacy law

The central recommendation of this Article is that lawmakers and regulators should force almost every company that handles customer information to associate its brand name with a specified set of core privacy commitments. The name, "Facebook," for example, should be inextricably bound to that company's specific, fundamental prom-

ises 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 be required to use a new name with its modified service, albeit perhaps one associated with the old name, such as “Facebook Plus” or “Facebook Enhanced.”

Although this solution is novel, it is far from radical when one considers how well it is 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, representing another important intradisciplinary bridge, this one between privacy law and product safety law. Just as companies selling inherently dangerous products are obligated to attach warning labels, so too should companies shifting to inherently dangerous privacy practices be required to display warning labels. And the spot at the top of every Internet web page listing the brand name is arguably the only space available for an effective online warning label. A “branded privacy” solution is also well-supported by trademark theory, which focuses on giving consumers the tools they need to accurately and efficiently associate trademarks with the consistent qualities of a service in ways that privacy lurches disregard.

At the same time, because this solution sets the conditions of 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 proper balance between the positive aspects of dynamism and the negative harms of privacy lurches. Companies will be free to evolve and adapt their practices in any way that does not tread upon the set of core privacy commitments, but they can change a core commitment only by changing their brand. This rule will act like a brake, forcing companies to engage more in internal deliberation than they do today about the class of choices consumers care about most, without preventing dynamism when it is unrelated to those choices or when the value of dynamism is high. And when companies do choose to modify a core privacy commitment, its new brand will send a clear, unambiguous signal to consumers and privacy watchers that something important has changed, directly addressing the information quality problems that plague notice-and-choice regimes in ways that improve upon prior suggestions.