Could Boucher Privacy Bill Stifle Innovation?

Mark Kesslen and Matthew Savare, Lowenstein Sandler PC

Think about how many times you've heard the word "reform" in the last year. Well, the federal government is on the verge of uttering it again, and this time concerning data privacy. For anyone following data privacy regulation, this news should come as no surprise, as the government has been talking of regulation for years. In an election year, when politicians from both sides of the aisle can demonize online advertisers as greedy companies hell bent on selling the most private information to the highest bidder, it is indeed an opportune time for lawmakers.

Specifically, over a year after promising to introduce new privacy legislation, Virginia Representative Rick Boucher unveiled a discussion draft (the "Draft Bill") of his proposed House bill on May 4, 2010. According to Boucher, the goal of the Draft Bill is to "encourage greater levels of electronic commerce by providing to Internet users the assurance that their experience online will be more secure." Despite this laudable goal, the Draft Bill, which is sweeping in scope and ambiguous in certain critical areas, does not deliver on its promise to improve data security. At best, it codifies many of the same self-regulatory principles adopted by the online advertising industry less than a year ago, which have not been given adequate time to address the perceived problems with online data privacy. In reality, the Draft Bill has the potential to increase transaction costs, stifle new innovation, and upset the very business model that allowed the Internet to flourish in the last decade.

Overview of the Draft Bill

Disclosure of Privacy Practices

The Draft Bill requires that any "covered entity"—defined as a company engaged in interstate commerce that collects "covered information" from more than 5,000 people in any twelve-month period or *any* "sensitive information"—conspicuously display a clearly-written privacy policy that explains a litany of things, including how information about individuals is collected, stored, used, merged with other data, disclosed, and discarded. The Draft Bill broadly defines "covered information" to include, among many other things, name; address; phone or fax number; e-mail address; biometric data; Social Security number, tax ID, driver's license number, or any other government-issued ID number; financial account information, including security codes and passwords; any unique persistent identifier, such as IP address; and preference profiles. The Draft Bill also broadly defines "sensitive information" to

---

mean information related to an individual's medical records, race, ethnicity, religious beliefs, sexual orientation, financial information, or precise geographic location information.

Significantly, the Draft Bill applies not only to covered information collected online, but also to any covered information collected offline. In such cases, the covered entity is required to make its privacy policy available to the individual in writing *before* collecting any covered information.

There are three important exceptions to this disclosure requirement. First, it does not apply to a "transactional purpose," which the Draft Bill defines as a "purpose necessary for effecting, administering, or enforcing a transaction between a covered entity and an individual." Second, "operational purposes" are exempted from the disclosure requirement. That term is defined as purposes "reasonably necessary for the operation of the covered entity," such as (1) providing, operating, or improving a product or service, (2) detecting, preventing, or combating threats against the covered entity, (3) disclosing data based on a law or regulation, or (4) sharing data with parent, subsidiary, or controlling companies.

However, the definition of "operational purposes" expressly excludes "marketing, advertising, or sales purposes, or any use of or disclosure of covered information to an unaffiliated party for such purposes."

Finally, covered entities may continue to collect and disclose "aggregate information," that is, information about a group of individuals that contains no personally identifying information, and data that has been rendered anonymous.

Collection and Use of Information

Aside from the exceptions listed below, the Draft Bill employs an opt-out regime, meaning that covered entities are permitted to collect covered information unless an individual affirmatively declines consent.

If an individual declines consent at any time, the covered entity may not collect covered information from that person or use covered information collected prior to the individual's opt-out. This provision is particularly controversial for advertisers, because it is a marked departure from the industry's current self-regulatory principles and the Federal Trade Commission's ("FTC") own guidelines, which do not require publishers or other "first parties" to allow opt-outs of data collection and use on their own sites. The ad industry, including the Interactive Advertising Bureau, has already decried this provision as an impediment to industry growth.

As noted, there are some very important exceptions to this opt-out regime. First, covered entities require an individual's express opt-in consent before collecting any "sensitive information" about an individual. Second, and especially contentious with the ad industry, is the requirement that if a covered entity wants to share an individual's covered information with unaffiliated third parties (other than for an operational or transactional purpose), the individual must grant affirmative consent for that sharing. Third, covered entities must obtain an individual's express affirmative consent before collecting or disclosing covered information about "all or

substantially all of an individual's online activity, including across websites." This practice, generally known as behavioral advertising, has come under increased scrutiny in the last several years, and the Draft Bill keeps the practice in the government's cross hairs. However, the Draft Bill contains an important exception to this general rule requiring opt-in consent for behavioral advertising. An opt-out system would apply if the covered entity (1) allows individuals to access and revise their profiles to opt-out, (2) deletes or renders anonymous any covered information within eighteen months after collecting the covered information, (3) prominently includes a symbol near any targeted ads that connects the individual to information regarding the ad network's data practices, and (4) does not disclose or allow its ad network to disclose this covered information to any other party without the individual's prior consent. Some companies that serve targeted ads, such as Google and Yahoo, already have this feature in place.

Implementation and Enforcement

As with many other privacy issues, under the Draft Bill, the FTC would be tasked to adopt rules to implement and enforce the measure. Although the Draft Bill precludes any private right of action, states may enforce the FTC's rules through their attorneys general or consumer protection agencies.

Next Steps

The Draft Bill's Executive Summary states:

> Broadband networks are a primary driver of the national economy, and it is fundamentally in the nation's interest to encourage their expanded use. One clear way Congress can promote greater use of the Internet is to assure individuals a high degree of privacy protection, including transparency about the collection, use and sharing of information about them, and to give them control over that collection, use and sharing, both online and offline.

Notwithstanding this claim, one wonders exactly how "clear" it is that government regulation of data privacy can truly promote increased usage of the Internet. Hasn't the Internet and all its complementary technological advances, including mobile platforms, flourished without comprehensive privacy legislation? Are many people really opting not to use the Internet because of the privacy practices of legitimate companies? Data breaches, identify theft, phishing, and all other sort of schemes are perpetrated by rogue individuals and organizations. When is the last time that an ad exchange caused such havoc? Representative Boucher and privacy advocates ignore the fact that online advertising, even behavioral advertising, does not—in and of itself—put data at risk or make it less secure. In fact, the largest data breaches have had nothing to do with what Representative Boucher now seeks to regulate. So, exactly how is the Draft Bill going to make individuals' data more secure? It isn't.

The government and privacy advocates alike have struggled to define the harm that flows from online behavioral advertising and increased information flow. They point to ill-defined concepts, such as loss of autonomy or control and paint all online marketers as irresponsible moneygrubbers willing to sell your most private

information for a buck. They downplay the utility of online advertising and the benefits of being digital.

There is no question that companies should respect the privacy of each and every individual. However, government regulation tends to throw the baby out with the bathwater, and the government has not even given industry the chance to self-regulate this issue. Remember, the ad industry just adopted its principles for behavioral advertising in July 2009.

Representative Boucher plans on soliciting comments to his Draft Bill over the next month or two. He then plans on sending a revised bill to the House Subcommittee on Communications, Technology, and the Internet, which he chairs. After that, the bill will make its way through the legislative morass. Although it may be many months before Congress votes on any version of this legislation, it continues to put a black cloud over the industry. For the sake of continued innovation and a free and vibrant Internet, let's hope most legislators opt-out of signing on.

Mark P. Kesslen runs IP for the Tech Group at Lowenstein Sandler and co-chairs the firm's IP Litigation Group. Prior to that he was Chief IP, Technology & Sourcing Lawyer worldwide for JPMorganChase. Matthew Savare specializes in privacy, IP, and media in Lowenstein's Tech Group and is a frequent author and lecturer on the subjects. Contact them at: mkesslen@lowenstein.com and msavare@lowenstein.com or on the web at www.lowenstein.com.