Davis Wright Tremaine LLP

An Advertising Perspective on the Kerry-McCain and Stearns-Matheson Privacy Bills

By Paul Glist

April 18, 2011

Last week, Sens. John Kerry and John McCain and Reps. Cliff Stearns and Jim Matheson offered new privacy bills. The Kerry-McCain Senate bill and the Stearns-Matheson House bill each seeks to apply a common set of fair information practices on virtually all businesses, online and offline, that collect information about consumers or consumer behavior. For the moment, both bills are directed to commercial and non-profit organizations (such as many online businesses) that are currently not under privacy regulation.

Kerry-McCain would also apply to the cable, satellite and telephone industries that to date have been governed by Cable Act privacy and CPNI rules. Neither bill would displace current privacy laws applicable to health, educational, credit and financial records, debt collection, children's online data, or the Electronic Communications Privacy Act (ECPA). As explained below, these new proposed laws could have a significant impact on advertising and advertising platforms.

Kerry-McCain bill

Background and framework

The Kerry-McCain bill would apply to any commercial or non-profit entity which collects, uses, transfers or stores "covered information" for more than 5,000 individuals a year. However, it applies this model only to organizations (such as many online businesses) that are currently not under privacy regulation; and to the cable, satellite and telephone industries that to date have been governed by Cable Act privacy and CPNI rules.

The bill's approach to what information is "covered" reflects a significant advance over prior formulations. The FTC's December 2010 Preliminary Staff Report and several earlier privacy bills were focused on online behaviorally targeted advertising, and therefore tended to treat device identifiers or de-identified information as if they were always personally identifiable. That approach not only undermined many advertising models that preserved anonymity, but also undermined business incentives to even bother protecting privacy by de-identifying information.

The Kerry-McCain bill tries to rectify this problematic formulation by applying privacy obligations to a wide set of "covered information," but distinguishing between classes of information. Information that by itself can identify a specific individual (or a mobile device number) is treated as "personally identifiable," and subject to elevated protections. Information associated only with a "unique identifier" is subject to protections appropriate to preserving anonymity or not "covered" at all. Extensive provisions for notice, choice, security, access, and accountability apply widely to covered data, but with more refinement than has been shown in prior bills. It does not

propose any “do not track” mechanism.

Effect on advertising

From the perspective of advertisers and advertiser-supported platforms, the Kerry-McCain bill is best understood through a few use cases.

- “First party” advertising and marketing from a website or subscription service—even if targeted based on “covered information”—is treated as a permissible part of ordinary business operations when using information collected by the entity providing the service. Profiles for first party ads may be enhanced by merging certain data sets—such as information which is shared by an advertiser with an established account and business relationship with a consumer.

- Consumers are provided more choices with respect to third party behavioral advertising and marketing. They must be provided an opportunity to opt-out of the transfer of both “personally identifiable” and anonymous profiles with “unique identifiers” for these purposes. Transfers to service providers and to third parties under common ownership or corporate control are permitted without an opt-out opportunity. Consumers must opt-in to allow collection and use of sensitive PII (discussed below).

- Analytics for internal use by the website or service provider would also be permitted, if reasonably described in privacy notices. Traffic and click-through data collected by websites are specifically permitted, both for improving website performance and navigation and “to understand and improve” the interaction of an individual with advertising. In addition, covered entities with an established business relationship are permitted any other data use which “the individual could have reasonably expected … , was related to a service provided” and is “reasonable and consistent with” disclosed practices and purposes. In all these cases, consumers are to have notice, but there is no mandatory opt-out requirement.

- Interactive transactional services—such as e-commerce, t-commerce, or requests-for-information—could largely operate in the ordinary course of business. Use of personally identifiable information to fulfill a requested transaction is authorized.

- Information voluntarily shared or authorized to be shared with unrestricted public forums, reported by the media, or dedicated to contacting individuals at work is not “covered information.” Public record information is also not “covered information,” unless merged with covered information from other sources.

Other FIPPs obligations

The Kerry-McCain bill, of course, includes a full suite of fair information practice principles (FIPPs).

Notice, Purpose Specification, Data Minimization and Retention. Notice is to be clear,

concise, timely, and state the "specific purposes of" data collection, use and transfer. Data may be collected not merely for fulfillment but also for marketing and advertising. Data may be retained for research and development even after an individual terminates service, but some PII is to be deleted or disabled if the entity possessing it files for bankruptcy.

Choice. Individuals may opt-out of the transfer of covered information (including unique anonymized profiles) for behavioral advertising or marketing. Individuals must opt-in to the collection, use or transfer of sensitive information. "Sensitive" is defined as information related to a particular medical condition, religious affiliation, or PII which if disclosed without authorization carries a significant risk of economic or physical harm.

Security, Accountability and Privacy by Design. All covered entities are required to protect covered information; to design privacy protections into their products, data processes and management processes; and to establish systems for responding to non-frivolous individual privacy complaints.

Accuracy, Access and Correction. Reasonable procedures should attempt to assure accuracy of PII if it "could be used to deny consumers benefits or cause significant harm." Each covered entity must also provide access and means to correct stored PII.

Preserving anonymity. The bill requires that transfers of de-identified data to third parties must include use restrictions and prohibit data merges seeking to re-identify individuals. The transferring party is also required to conduct due diligence on the legitimacy and reliability of the transferee. The transferee is then treated as a covered entity, unless the FTC grants an exception.

Enforcement. The FTC serves as the enforcement authority. If the FTC has not acted, State Attorneys General may also bring civil actions on behalf of State residents to address "economic or physical harm" or other violations. Civil penalties are capped at a maximum of $3 million for any related series of violations. No private causes of action are allowed. State laws are preempted, other than laws concerning health information, financial data, data breach, and fraud.

FTC rulemaking

The FTC is given rulemaking authority to define virtually all of these FIPPs elements, but there are significant limitations. For example, security regulations must be consistent with recognized industry practices today, and proportional to the size, type, and nature of covered information. Nor may the FTC prescribe any specific product, technology, software or hardware.

Safe harbor

The bill anticipates a role for self-regulatory safe harbors run by FTC-approved non-governmental organizations. These would provide easy mechanisms for consumers to opt-out from data transfers to third parties for behavioral advertising, location-based ads, and other uses. They would also offer protections equivalent to the statutory requirements for notice, choice, data minimization, third party contracts, and accuracy.

Safe harbor participants would remain subject to the bill's requirements for accountability, privacy by design, and enforcement.

Commerce Department

As contemplated by the Commerce Department's Privacy Green Paper, the Commerce Department would also convene stakeholders to develop safe harbor codes of conduct; to promote international interoperability; and to conduct research in areas such as anonymization of data.

Stearns-Matheson bill

The Stearns-Matheson bill has a less regulatory orientation. While it covers the usual FIPPs territory, it makes significant improvements in several areas that have proven problematic in earlier draft bills.

- It explicitly treats anonymized data and inferred profiles as not "personally identifiable."
- It facilitates innovative uses of data by allowing privacy notices to describe the "types" of purposes and uses anticipated, and allows new uses to be made on notice. Other bills have tended towards great specificity in purpose limitations and opt-in requirements for later changes in use.
- It is less formulaic in defining corporate affiliates, allowing first parties to build their network of affiliates with contracts that require security and privacy protections.
- It requires that consumers be given rights to opt-out, but only when PII is transferred to unaffiliated third parties.
- It provides much more detail for establishing and operating self-regulatory safeharbors.
- Enforcement procedures favor rapid private arbitration, with possible appeals to the FTC, and civil penalties are capped at $500,000 for all related violations.
- It preempts private causes of action and state and local privacy rules.

However, as noted above, the Stearns-Matheson bill seeks to apply this model only to businesses (such as online businesses) that are currently not under privacy regulation.

The existing laws governing the cable, satellite and telephone industries, health, educational, credit and financial records, debt collection, children's online data, and ECPA would remain intact.

This advisory is a publication of Davis Wright Tremaine LLP. Our purpose in publishing this advisory is to inform our clients and friends of recent legal developments. It is not

intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.