KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

CDT TOP-LEVEL ANALYSIS OF THE COMMERCIAL PRIVACY BILL OF RIGHTS ACT OF 2011

April 27, 2011

On April 12, Senators John Kerry of Massachusetts and John McCain of Arizona introduced the "Commercial Privacy Bill of Rights Act of 2011" to provide long-needed protections around the collection, use, and transfer of consumer data. Below we offer some initial thoughts on some of the key provisions in the bill.

On April 12, Senators John Kerry of Massachusetts and John McCain of Arizona introduced the "Commercial Privacy Bill of Rights Act of 2011" to provide long-needed protections around the collection, use, and transfer of consumer data. The bill places substantive requirements on covered entities reflecting each of the Fair Information Practice Principles: security (§101), accountability (§102), transparency, purpose specification, and use limitation (§201), individual participation (§202), data minimization (§301), and data integrity (§302). The bill also contains a provision requiring companies to implement the principles of "Privacy by Design" throughout a product's lifecycle (§103).

The Federal Trade Commission and state Attorneys General are authorized to enforce the bill's provisions and obtain injunctive relief and statutory penalties from violators. However, the bill also provides for the development of privately-run "safe harbor programs" (§501(a)); any participating company in compliance with a such a safe harbor program is deemed to be in compliance with most the bill's provisions (§502(a)). The Federal Trade Commission must give formal authorization to any safe harbor program and maintains supervisory authority over the operation of such programs (§501(b), (d)). The Department of Commerce is authorized to convene multi-stakeholder negotiations in developing safe harbor programs (§701), though putative programs may also simply apply directly to the FTC for safe harbor status.

STRENGTHS OF THE KERRY/McCAIN BILL

A. The bill implements the full range of Fair Information Practice Principles for all consumer data

The Kerry/McCain bill incorporates the full range of Fair Information Practice Principles (see above) and applies them to all companies (and nonprofits) that collect and use personal information—either online or offline. Privacy advocates have long called for such comprehensive, baseline protections for consumer data to fill in the gaps created by the noncontiguous patchwork of sector-specific laws we have today.

The bill also applies not just to traditional "personally identifiable information," such as name, email address, or social security number but to a broader range of personal information (called "covered information" under the bill) as well, including profiles tied to a pseudonymous identifier (such as a cookie or IP address). The bill applies most of the same protections to the broader range of covered information as it does to "personally identifiable information, though not the rights of access and correction to profile information. The bill does provide for the right for consumers to access any "personally identifiable information" that the company possesses about an individual (§202(a)(4)), though we would recommend that that right be extended to include any other profile information about the individual that a company associates with a "personally identifiable" profile.

B. The FTC is charged with developing standards for notice

The bill gives the Federal Trade Commission ("FTC") the authority to promulgate rules for how consumers should be given notice of what data is collected, how it is used, and to whom that data is transferred (§201). This would be a considerable improvement over the present unregulated "notice-and-choice" approach, under which many companies reserve broad rights to use consumer information in arcane (and mostly unread) privacy policies, and consumers are presumed to have consented to such usage under the law. Giving the FTC the discretion to determine and change over time as appropriate the standards which notice must meet under the act makes more sense than to statutorily require a long list of required information in a privacy policy (as was the case under previous privacy bills.). In its recently draft privacy report, the FTC issued intelligent, workable guidelines for offering consumer more meaningful "just-in-time" notices to afford them a greater understanding of how their data is managed and shared. Giving the FTC the authority to embody those guidelines in enforceable regulation would give greater certainty to companies, better notice to consumers, and the flexibility to update the guidelines in response to new technical and market developments.

C. The bill creates a flexible safe harbor framework

The bill provides for flexible and practical implementation of the Fair Information Practices through safe harbor programs developed through multi-stakeholder negotiation (§§501-02, 701), as envisioned under the Department of Commerce "Green Paper" privacy report and approved by the FTC. The bill gives the Department of Commerce the authority convene businesses, civil society, and academia to develop industry-specific rules. Industry groups can also petition the FTC for approval of codes designed on their own. CDT believes that such a consensus-based, narrowly-tailored approach can most effectively bridge the gap between the high-level privacy principles in the bill (such as "individual participation" and "data minimization") and meaningful on-the-ground implementation across diverse business lines.

As we read it, the bill also requires that safe harbor programs establish a global opt-out mechanism for the transfer of covered information to third parties for unauthorized uses (§501(a)(2)), though that language could be clarified. In a choice environment predicated upon opt-out, as opposed to opt-in permissions, consumers need the ability to signal choices to wide swaths of industry participants at once, rather than have to identify the potentially hundreds of companies collecting and using third-party data about them. We believe global opt-out choices (such as "Do Not Track" in the online behavioral advertising environment) are effective mechanisms for consumers to exercise control of their personal information, though only if all there are sufficient incentives to drive all industry participants into a safe harbor program (on that, see below).

D. The FTC and state Attorneys General can impose significant penalties upon wrongdoers

The bill authorizes regulators to obtain civil penalties of up to $6 million for some (but not all) of the bill's substantive protections (§404). To date, the FTC and the states have brought a number of important privacy cases, such as recent settlements against companies who offered deceptive and ineffective opt-out solutions, and against Google for sharing personal data with other Google customers in violation of previous representations as part of the Buzz product. While these cases are important, they also demonstrate that the FTC is generally limited under current law to bringing enforcement actions against companies makes affirmative misstatements about their own privacy practices. In order for the privacy protections in this bill to be meaningful, enforcers will need the authority to deter illegal practices and punish those who engage in those practices.

E. The bill includes a reasonably scoped "right to be forgotten"

While the United States is debating how to implement a comprehensive privacy framework for the first time, in Europe, which has long had a Data Protection Directive, recent debate has centered on "The Right to be Forgotten." The idea behind such a right is that you should be able to exercise control over your privacy by removing embarrassing information about yourself from the internet. In some jurisdictions, the expression of this right has taken an extreme turn, and CDT has argued against the application of this right to require search engines and news reporters to erase perhaps uncomfortable facts from the web.

The Kerry/McCain approach, however, is narrowly scoped to afford consumers a right to delete information from companies with which they have a direct service relationship (§202(a)(5)). CDT has previously argued for an interpretation of the right to be forgotten as the ability to delete data that an individual has affirmatively put into the cloud. The Kerry/McCain formulation should be slightly modified to similarly address data that users put into a public forum or social networking site (though not for that data as repurposed by others). However, the deletion requirement should perhaps be narrowed to that data which the consumer directly provided to the company.

II. SUGGESTED REVISIONS

A. The definition of "third party" should be expanded to includes non-commonly branded affiliates and companies with which a consumer has an "existing business relationship"

One significant concern CDT has with the Kerry/McCain bill is its extremely narrow definition of third parties (§3(7)). The distinction is significant, because first parties are exempted from certain requirements in the bill; most notably, first parties do not need to allow consumers any choice over whether and how their information is used for first-party marketing. Wholly exempting first-party marketing from user control is concerning in its own right, but the bill further compounds this problem by significantly expanding the definition of first-party.

First, the bill interprets all parties under common corporate ownership or control as first parties (§3(7)(A)). Thus, large diversified businesses with separate — and from a user's perspective,

distinct — business lines would be able to merge consumer data across first parties without user consent (either opt-in or opt-out). For example, IAC Interactive Corp. owns and operates dozens of popular and seemingly unrelated sites, such as Thesaurus.com, College Humor, Match.com, and Urban Spoon, would be able to track users across those domains without user control. CDT believes that first party transfers should be limited to those companies that operate under a common brand, or otherwise where an ordinary consumer would understand that the two business lines were owned by the same company.

The bill also allows any entity with which a consumer has an "established business relationship" to operate as a first party regardless of context — so long as the company clearly identifies itself at the time of collection (§3(7)(C)). Modern webpages often incorporate any number of third parties onto their site (a Wall Street Journal inquiry found 159 third-party cookies on the site Dictionary.com); under the Kerry/McCain formulation, any site with which a user has a preexisting relationship can completely avoid any consumer control over the collection or use of information so long as the party clearly identifies itself (only the disclosure of the presence of the company is required, not the fact of information collection). Social widgets or branded ads by membership sites like Facebook, Twitter, LinkedIn, Google, Reddit, Yahoo!, and so on all could claim the right to track users without offering choice. Indeed, such an exception could push standard practice on the web to always logged-on or real-name environment, which was precisely what the FTC was concerned about when it raised objections to the DoubleClick-Abacus merger in 2000 over the merger of identifying data with clickstream data. If all sites are encouraged to gather identifying information from consumers, this would present a very strong threat to privacy and free speech online.

A consumer's web experience is often improved by the incorporation of third-party content — even personalized third-party content — and data privacy legislation should be flexible enough to allow third-party services to render such content — even personalized content — without tracking users across multiple domains. However, by defining a party with which you have a first-party relationship in *some* contexts as a first party in *all* contexts deprives users of too much control of their personal information in the bill's current form.

B. The bill should provide stronger incentives to companies to join safe harbor programs

As noted above, CDT believes that FTC-approved safe harbors are a smart, flexible means to implement privacy protections across a range of divergent industries. But for them to be attractive to companies, legislation has to encourage companies to participate in safe harbor programs by exempting them from requirements. For example, Rep. Rush's BEST PRACTICES bill first introduced last year encouraged companies to join a safe harbor by exempting participants from opt-in permission for sharing personal information with third parties, and the private right of action. Under the Kerry/McCain bill, strong incentives like a private right of action and opt-in permission for sharing are not included, (§§ 202(a)(1)-(2), 406) . There are convincing arguments for including those provisions in their own rights, but if nothing else they should be included in the bill as defaults for companies that fail to join self-regulatory programs, and as powerful incentives to companies to participate in the Department of Commerce-led multi-stakeholder meetings to develop strong and enforceable industry-specific privacy protections.

Parties who join safe harbor programs under the Kerry/McCain bill are deemed to be in compliance with the substantive provisions of the law, provided that compliance with the safe harbor status must be at least as strong as the underlying law. As such, it is difficult to see the

incentive for most companies to join such a program. The Children's Online Privacy Protection Act ("COPPA") has a similar safe harbor structure, with "deemed compliance" as the only benefit for participation. Only a handful of companies have sought to join a COPPA safe harbor program. Similarly, Article 28 of the European Data Protection Directive allows for participation in industry-supported "codes of conduct" to achieve compliance under the law; those safe harbor programs have also been very undersubscribed. We believe this bill is forward-looking in envisioning that the development of industry-specific rules could be achieved through co-regulatory safe harbor programs, but the current iteration of the bill does not provide sufficient incentives to ensure that such programs will be widely adopted or meaningful. Opt-in permissions for sharing and a private right of action should be included in the Kerry/McCain bill as a default in order to encourage all industry players to join the multi-stakeholder development of robust safe harbor regimes.

C. The bill should provide for general FTC rulemaking, especially around definitions

Although the FTC is given the ability to promulgate regulations on specific sections of the bill (§§101(a) (security), 201(a) (transparency), 202(a) (choice), 501(a) (safe harbors)), generally speaking the FTC is not allowed to issue clarifying rules under this bill. This impinges on the bill's ability to stand the test of time, as new scenarios may emerge that require clear standards for companies to stay compliant with the law. While we expect that much of these standards can be implemented through the safe harbor programs, the FTC needs the ability to issue rules for those gaps that the safe harbor programs do not address.

The definitions of "personally identifiable information" and "sensitive information," for example, should certainly allow for FTC rulemaking, as what could be reasonably linked back to a person and what data we consider "sensitive" (and deserving of stronger protections) may well change over time. Currently, the bill merely defines "sensitive information" as that which carries a significant risk of harm; this does not provide companies much certainty in evaluating what levels of protections certain categories of data need (the bill separately defines certain medical and religious information as "sensitive," though those terms could also benefit from clarification). The Kerry/McCain bill should grant the FTC the authority to issue implementing regulations for all of the bill's provisions in order to respond to technological and marketplace evolution

D. The bill should provide consumer control for third-party collection of data, not just usage

By and large, the Kerry/McCain bill only governs the *use* of personal information by companies (including third parties), and offers consumers few rights as to the collection of that data in the first place. Under such a regime, innumerable third parties can obtain and store user data outside the consumer's control, subject to potential data breach, government access, or illicit usage. Certainly, those extra parties would be subject to the bill's data minimization requirements (§301), but historically data minimization has been the most challenging of the Fair Information Practices to implement, and Section 301 currently has numerous, broad exceptions, and is not subject to FTC rulemaking or state Attorney General enforcement. Given legitimate concerns about the strength of this provision, consumers should be allowed to exercise control over the transfer of their information to third parties for "unauthorized" purposes. Transfers to third parties for common and expected purposes are already allowed under other provisions of the Act (§§3(8), 202(a)(1)-(2), 202(d)).

E. The bill should require a full range of enhanced Fair Information Practice Principles for all "sensitive information," not just personally identifiable sensitive information

Although the Kerry/McCain bill provides for consideration of the sensitivity of information in the development of appropriate security protections (§101(b)), the implementation of the other Fair Information Practice Principles do not consistently reflect that sensitive data merits greater protection. The bill does provide for heightened opt-in permission before the sharing of sensitive "personally identifiable information," but does not extend such permissions to the use of sensitive information attached to pseudonymous profiles for unauthorized purposes, including marketing (§202(a)(3)(A)). Existing industry standards by groups such as the Network Advertising Initiative already require opt-in consent for the use of sensitive information in marketing. We believe that the bill should require consideration of the sensitivity of consumer information in the implementation of each substantive provision, for both real-name and pseudonymous profiles tied to a unique identifier (such as a cookie).

F. The bill should not weaken the FTC's long-established requirement to obtain affirmative opt-in consent before making material changes in privacy policies

The Federal Trade Commission and courts have consistently interpreted the FTC's existing Section 5 authority (prohibiting unfair and deceptive business practices) to prohibit companies from changing privacy policies and retroactivity treating previously collected data pursuant to the terms of the new policy. This prohibition makes sense, as it would render any assertions or promises under such a policy illusory, as a company could simply change the terms at will later on. Under existing law, companies may only get around this prohibition if consumers give their affirmative opt-in permission to have their data treated pursuant to the new terms. The Kerry/McCain bill only requires such opt-in consent if a new "use or transfer creates a risk or economic or physical harm to an individual." (§202(a)(3)(B)) Covered entities should not be given free rein to revoke their privacy representations and promises to consumers so long as consumers are not at risk of injury

G. The bill should require entities who collect and use all or substantially all of a consumer's online activity for unauthorized uses to obtain opt-in consent to do so

Another concern about the bill is that there is no requirement that ISPs, browsers and other entities that collect "all or substantially all" of a consumer's online activities for behavioral advertising (or other unauthorized uses) obtain opt-in consent from the consumer. That requirement is included in the FTC behavioral advertising report and reflected in current self-regulatory programs. This omission is exacerbated by the fact that the bill eliminates the existing rules for cable and telecommunications in the Communications Act and replaces them with the lesser protections of this baseline bill (§601(c)). Thus, phone and cable companies whose privacy practices are currently regulated by the FCC and who must get affirmative opt-in permission to share customer data with third parties would under Kerry/McCain only require companies to offer to consumers the ability to opt out of personal information sharing under the supervision of the less prescriptive FTC. Under some interpretations of the bill, telecommunications providers could even be deemed "first parties" under the act, relieving them of any consent requirement. While CDT is sympathetic to the argument that as industries and mediums merge, the strong dichotomy in protections between carriers and the virtually nonexistent requirements on the rest of the industry needs to be addressed, the bill is simply not strong enough to warrant the loss of existing protections, and it fails to consider the implications of the change on other industries such as behavioral advertising and location-based services.

H. The bill should provide for narrowly-tailored preemption of state privacy laws only if it provides sufficient levels of protections for consumer data

CDT believes that preemption of state law in federal privacy law should be narrowly tailored to reach only those state laws that expressly cover the same set of covered entities and same set of requirements. States should be free to legislate in areas that the federal law was not intended to reach. Even then, CDT only supports preemption if the federal law provides as much protection as the best state laws. We do not believe that the current iteration of the bill is strong enough to preemption that would preclude states from adopting additional protection.

III. CONCLUSION

The introduction of the principled, bipartisan Kerry/McCain privacy bill represents a tremendous advancement in the long fight for the enactment of a baseline privacy law. While not perfect, the bill presents an opportunity to develop a strong, comprehensive, and flexible privacy protection framework that consumers and businesses increasingly need in the modern data ecosystem. CDT urges industry and civil society groups to take advantage of this opportunity by constructively engaging with the drafters and the members of the Senate Commerce Committee in refining and improving this bill and advocating toward its eventual passage.

For More Information

Please contact:

Justin Brookman
Director of CDT's Consumer Privacy Project
202.407.8812