May 25, 2010

The Honorable Rick Boucher
Chairman, Subcommittee on Communications, Technology and the Internet
House Committee on Energy and Commerce
2187 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cliff Stearns
Ranking Member, Subcommittee on Communications, Technology and the Internet
House Energy and Commerce Committee
2370 Rayburn House Office Building
Washington, D.C. 20515

Dear Representatives Boucher and Stearns:

On behalf of the Information Technology & Innovative Foundation (ITIF), I urge you to consider refining the discussion draft data privacy legislation in order to create a more open data sharing environment that can allow continued innovation for online services.

As you may know, ITIF is a non-profit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Recognizing the vital role of technology in ensuring American prosperity, ITIF focuses on innovation, productivity, and digital economy issues.

As consumer data increasingly is collected and stored electronically, it is important for Congress to consider the effect this has on privacy. The discussion draft legislation provides a welcome opportunity to explore the best ways of protecting individual privacy while avoiding constraints on business innovation and unintended negative impacts on consumers. However, much of the concern over data privacy is speculative and consumers have experienced few, if any, harms because of the current privacy laws. Before Congress enacts new laws, it should first demonstrate that better enforcement of existing privacy regulations are insufficient to protect consumers. Enactment of this legislation as drafted would add yet another layer of complexity to the existing patchwork of federal laws regulating consumer privacy, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA) and the Fair Debt Collection Practices Act

(FDCPA). Too often such legislation ends up imposing news costs on consumers and limiting innovation and the development of new online services.

This is not to say that a federal framework for consumer privacy would not be useful. One particularly positive element of this draft legislation is that it includes a preemption clause so that the proposed federal law would supersede any state regulations. To be effective, a federal framework for consumer data privacy should establish a single, nationwide standard for consumer privacy thereby reducing regulatory complexity for the private sector. If Congress does move forward with privacy legislation, it should ensure that any new regulations preempt state laws, otherwise online service providers will find themselves facing competing, and possibly contradictory, data use and handling requirements for consumers.

However, in its present form the draft legislation raises various concerns, outlined below. We recommend the following:

1. Eliminate provisions that raise costs for consumers while creating few benefits

The draft legislation includes certain provisions that create unnecessary costs for the private sector which will be borne by consumers that should be eliminated.

First, in an effort to apply the rules not just to the Internet, the draft legislation mandates that, in certain instances, organizations provide offline notification of their privacy policy to consumers. The legislation states, "If the covered entity collects covered information by any means that does not utilize the Internet, the privacy notice required by this section shall be made available to an individual in writing before the covered entity collects any covered information from that individual." The potential impact of this one sentence could be substantial as it would likely require many organizations to provide paper-based copies of their privacy policy to individuals. For example, this requirement would appear to limit the ability of organizations to collect registration forms or surveys from in-person events such as conferences or sporting events without first providing copies of the organization's privacy policy. Not only would this requirement cost a significant sum of money to implement nationwide, it would also be a waste of paper.

Second, the draft legislation mandates that all organizations covered under the legislation (i.e. virtually all online businesses) must have a privacy notice on their website conforming to specific requirements. The legislation defines 15 specific items that each privacy policy must contain including, for example, "a hyperlink to or a listing of the [FTC's] online consumer complaint form." While privacy policies have

been an industry best practice for many years, this legislation would impose a cost on organizations large and small as they would need to undertake a review of their privacy policy to ensure it conforms to this legislation and yield negligible benefits to consumers. Legislation should not require organizations to have a privacy policy or require specific elements in a privacy policy because existing mechanisms, such as industry self-regulation and consumer-friendly tools such as the TRUSTe privacy seal, provide sufficient and more effective protection for consumers. In addition, much of the criticism about the complexity of online privacy policies is unfounded, because many of these privacy policies are supplemented by additional online content (e.g., a Frequently Asked Questions page) which explains the privacy practices of an organization in plain English. Federal effort in this area should be focused on more rigorous enforcement of privacy policies and better consumer education.

2. Do not establish affirmative consent ("opt in") requirements for the collection, use and disclosure of certain types of information

Currently, organizations operate under a notice and choice regime, whereby consumers can review the privacy policies, if any, offered by an organization, and then decide whether to use the services offered by that organization. For example, if a new mobile application or online service does not provide a privacy notice on their website, consumers can decide that this does not meet their standards and not use the application or service. While many privacy advocates would like to see a more granular system in which consumers could opt out of specific types of data collection and use, the current privacy regime is effectively an opt-out system since consumers can decide whether or not to use a service based on the data usage and handling practices of an organization.

The draft legislation ends the current regime by establishing affirmative consent ("opt in") requirements for certain situations including: collecting sensitive information and location-based information; sharing information with third-parties; and modifying an organization's privacy policy. Others have shown how "opt-in is a rhetorical straw-man that cannot really be implemented by regulatory policies without creating a number of unintended side effects, many of which are suboptimal for individual privacy."[1] In addition, opt-in requirements create an administrative burden on organizations as they must ensure that every user take a proactive step before they can offer their customers a specific service. Policymakers should endeavor to understand the costs of opt-in before enacting this requirement.

[1] Nicklas Lundblad and Betsy Masiello, "Opt-in Dystopias," *SCRIPTed* 7, no. 155 (2010), http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

For example, the draft legislation unnecessarily restricts the collection of certain types of information related to an individual's location or deemed "sensitive." Societal values change over time and privacy is no different. Over the course of human history, privacy itself is a relatively new value, and varies from culture to culture (and person to person). Certainly the last decade has seen a sharp rise in individuals willing to share what was previously considered private information publicly on the Internet. In particular, the draft legislation sets unique requirements for what it deems "sensitive" information. The legislation defines sensitive information as data that relates to an individual's medical information, race or ethnicity, religious beliefs, sexual orientation, finances, and precise physical location. Legislation should not codify existing social norms at the expense of future innovation.

In addition, the restriction on sharing information with third parties would limit the ability of organizations to integrate their services with other providers. For example, organizations would find it more difficult to partner with outside entities to create a combined service. Mash-ups—remixing data across multiple external service providers—are one of the hallmarks of the Web 2.0. Organizations using services provided by another entity that require consumer information, for example an online mapping service, would possibly not be allowed without affirmative consent. Similarly, the requirement that covered entities obtain affirmative consent from users before making any material changes in their privacy policies would restrict the ability of service providers to rapidly develop and deploy new services, such as the changes recently introduced by Facebook.[2] These types of restrictions would effectively create speed bumps to innovation.

Finally, by requiring organizations to obtain affirmative consent for every material change in their privacy policy, this legislation would create an incentive for organizations to establish unrestrictive privacy policies so that future development would not be needlessly constrained by their own policies. The opt-in requirements should be eliminated from the proposed legislation.

3. Eliminate restrictions on behavioral target advertising

While ITIF welcomes the support some members of Congress have shown for behavioral targeted advertising, the draft legislation includes certain provisions that would restrict this beneficial type of online advertising which provides consumers more relevant ads.

---

[2] Daniel Castro, *The Right to Privacy is Not a Right to Facebook* (Washington, DC: The Information Technology & Innovation Foundation, April 30, 2010), http://www.itif.org/publications/facebook-not-right.

First, the restriction on the collection and disclosure of certain types of information categorized as "sensitive" means there is an entire class of targeted advertising that cannot be used without organizations first obtaining affirmative consent. In particular, the restrictions on using data related to medical information, sexual orientation, race or ethnicity, and religious beliefs without affirmative consent would restrict many types of potentially beneficial forms of advertising. For example, these restrictions could potentially prevent marketers from effectively creating targeted ad campaigns for services like online Christian bookstores, Brazilian music stores, or gay dating websites.

Second, the draft legislation requires organizations to follow specific guidelines regarding the use of data in profiles used to provide services such as targeted advertising. For example, the legislation requires organizations to provide "a readily accessible opt-out mechanism whereby, the opt-out choice of the individual is preserved and protected from incidental or accidental deletion." This requirement goes against current industry practice. The Network Advertising Initiative (NAI), the online advertising industry organization that has been developing most of the standards for third-party ad networks, currently use cookies (small data files stored on a user's computer) to allow consumers to opt out of participating online advertising networks' behavioral advertising programs.[3] However, cookies do not fit the technology requirement as stated in the legislation since they can be accidentally deleted by a user, and so these third-party advertising networks would not be in compliance with the new legislation.

The legislation also requires websites to place a "symbol or seal" near every targeted ad that links to information about their advertising partner and information about any data associated with that user profile. Requiring targeted ads to have a special mark identifying them as such would unfairly disadvantage targeted ads against non-targeted ads. Given that targeted ads generate more than two times the revenue of non-targeted ads, this would have a negative impact on revenues for online publishers and service providers and would harm the Internet ecosystem, particularly the so-called "long tail" of small websites supported by ad revenues.[4] In addition, policymakers concerned with the decline of print media should note that greater revenue from targeted online advertising will likely be necessary for journalism to survive in the Internet age.

---

[3] "Opt Out of Behavioral Advertising," Network Advertising Initiative (2010), http://www.networkadvertising.org/managing/opt_out.asp.

[4] "Study finds behaviorally-targeted ads more than twice as valuable, twice as effective as non-targeted online ads," Network Advertising Initiative, press release, March 24, 2010, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf.

The legislation also states that users should be able to "review and modify" any preference profile created by an online ad network or other service provider. This requirement would force websites to build front-end systems to allow consumers to interact with data saved in their profile. Currently if consumers want to "opt out" of targeted advertising, they avoid websites that use this form of advertising or use various technical controls, such as web browser plug-ins, that block ads. This requirement would pose an unnecessary and unneeded cost on service providers (and ultimately consumers) and would generate little to no real benefit to consumers. Users that choose to opt out of targeted advertising but still access a website's content or services are free riders, getting all of the benefits of a free service without bearing any of the costs. It does not make sense to require service providers to build a system to make it easier for users to free ride by opting out of targeted advertising. Unfortunately, this type of requirement reflects the prevailing message of privacy fundamentalists that privacy trumps all other values. However, policymakers should recognize that privacy, as with any other value, must be balanced against other competing interests and can, as it will here, comes at a real financial cost.

4. Eliminate the provision that grants the FTC the authority to establish a security standard to protect consumer information

The draft legislation grants the FTC authority to "establish, implement, and maintain appropriate administrative, technical, and physical safeguards" that it deems necessary. Such a broad authority over every nongovernmental organization maintaining consumer information effectively gives the FTC a far reaching authority over the information security practices of the private sector. Using this authority, the FTC could effectively set the standard for the security practices of private sector systems and networks. While the federal government does have a role in fostering good information security practices, the private sector is in a better position than the federal government to manage risk for its own systems and networks. The FTC should not be granted this wide-reaching authority.

5. Include government use of digital data in any update to privacy laws

While the draft legislation attempts to enhance privacy for consumers, no mention is made of government use of consumer data. The draft legislation exempts government agencies from maintaining the same privacy standards that it would require from the private sector. Improper use of consumer data by government is arguably the greater threat preventing more widespread use of technologies like cloud computing. Privacy legislation should address government use of data to assure consumers that data government will not misuse personal data. As ITIF and others have argued previously, Congress should act to reform laws such as the Electronic Communications Privacy

Act (ECPA) to ensure that citizens have a right to privacy for their electronic data whether it is stored at home on a PC or remotely in the cloud.[5]

6. Protect and promote beneficial uses of information sharing

Finally, policymakers should recognize that consumer privacy should not come at the expense of beneficial uses of individual data. Both for-profit and non-profit organizations collect, share and use individual data routinely to provide important services. Organizations routinely purchase contact lists from companies like Hoover's to find sales prospects and media contacts. Websites like Trulia and Zillow use public databases to collect and share home prices and property tax information. Non-profits and politicians routinely purchase data for outreach and fundraising. Organizations promoting government openness use personal data to provide online tools to foster transparency and public accountability. For example, websites like OpenSecrets.org track money in politics and the website LegiStorm provides salary information on Congressional staffers. And of course many organizations have begun to use personal data for targeted advertising. Federal data privacy legislation should ensure that beneficial uses of data are not curtailed by overly-restrictive data sharing policies.

I urge you to consider carefully the concerns outlined here. Thank you for your consideration.

Respectfully Submitted,

Daniel Castro

Senior Analyst
The Information Technology & Innovation Foundation
1101 K Street NW, Suite 610
Washington, DC 20005
Phone: (202) 626-5742
Email: dcastro@itif.org

[5] "ITIF Calls for Updates to Privacy Laws," Information Technology and Innovation Foundation, press release, March 30, 2010, http://itif.org/pressrelease/itif-calls-updates-privacy-laws.