

January 28, 2011

National Telecommunications Administration  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Washington, DC 20230

**Comments of Consumers Union to the Department of Commerce Internet Policy Task  
Force on  
“Commercial Data Privacy and Innovation in the Internet Economy:  
A Dynamic Policy Framework”**

Docket No. 101214614–0614–01

**INTRODUCTION**

Consumers Union (CU),<sup>1</sup> the non-profit publisher of *Consumer Reports*®, supports the Department of Commerce’s (DOC) focus on developing stronger privacy mechanisms for commercial data. As noted by the DOC, the Internet and information technology have become integral to economic and social life in America and throughout the world. This technology has led to the growth of digital commerce, has enabled new forms of civil participation, and has transformed social and cultural bonds. Rapidly changing technological advances are often extremely beneficial to consumers, allowing individuals to receive relevant and timely information, complete transactions online, and interact with a global community. This free flow

---

<sup>1</sup> Consumers Union of United States, Inc., publisher of *Consumer Reports*®, is a nonprofit membership organization chartered in 1936 to provide consumers with information, education, and counsel about goods, services, health and personal finance. Consumers Union’s publications and services have a combined paid circulation of approximately 8.3 million. These publications regularly carry articles on Consumers Union’s own product testing; on health, product safety, and market place economics; and on legislative, judicial, and regulatory actions that affect consumer welfare. Consumers Union’s income is solely derived from the sale of *Consumer Reports*®, its other publications and services, fees, noncommercial contributions and grants. Consumers Union’s publications and services carry no outside advertising and receive no commercial support.

of information, however, can also jeopardize consumer privacy, resulting in decreased consumer trust and slower adoption of new online services.

CU is encouraged by DOC's recognition that trust is of central importance to the full use of the Internet as a political, educational, cultural, and social medium. In today's largely unregulated Internet environment, consumers face a continuum of risks to personal privacy, ranging from minor nuisances to improper disclosures of sensitive information and identity theft. Such unscrupulous practices, carried out without the consumers' knowledge or consent, lead to diminished consumer trust in Internet data practices, thus stunting growth and innovation. So far, industry self-regulatory initiatives, based primarily on the notice-and-choice system, have proven difficult and unwieldy for consumers, and have done little to restore confidence in the system. Few consumers have the capacity to sift through and fully understand lengthy privacy policies for each and every business entity they interact with online, in order to make informed decisions about how to best protect their personal information. If online privacy protections are ever to be truly meaningful, consumers cannot be asked to bear the sole burden of protecting the privacy of their data.

Consumers Union supports the adoption of a privacy framework that will protect consumer data both online and offline. This framework should be comprehensive, but not limiting, so that it can remain relevant in the face of constant technological innovation. CU believes this comprehensive privacy framework should be grounded in statute and implemented primarily by the Federal Trade Commission (FTC), an independent agency with a focus on protecting consumer rights. In addition, CU agrees with DOC that the Commerce Department,

working through the proposed Privacy Policy Office (PPO), could serve a key role in this process by helping to bring together many stakeholders interested in strengthening commercial data privacy protections. However, it is imperative that this process take into account consumers' interests in a meaningful way. Any stakeholder convening should include not only business groups but also representatives from consumer and privacy organizations.

Setting in place clear and certain baseline privacy principles will protect consumers while also addressing industry's need for predictability and clarity, thus spurring growth.

**RECOMMENDATION #1: Adoption of a Baseline Privacy Framework Based on Expanded Fair Information Practice Principles**

Consumers Union believes that any comprehensive baseline commercial data privacy framework must be grounded in statute. Such legislation, built upon an expanded set of Fair Information Practice Principles (FIPPs) would address consumers' privacy concerns while also enabling legitimate business and providing clear guidelines for industry. As noted in the DOC Green Paper,<sup>2</sup> businesses need certainty when it comes to the legal framework for privacy. Providing such clarity by legislation would reduce risk and uncertainty, leading to greater consumer trust and reducing business costs. The baseline legislation should also be broad enough to ensure that it can be adapted and applied to emerging technologies.

---

<sup>2</sup> See The Department of Commerce Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," p. 24. [hereinafter '*DOC Green Paper*']

The baseline privacy legislation should grant the Federal Trade Commission (FTC) extensive rulemaking authority to implement the directives of the legislation. As an independent agency with a focus on protecting consumer rights, the FTC should occupy a primary role in creating and enforcing standards and regulations based on the statute. The FTC should also be given flexibility to adapt the interpretation and implementation of the law to new and innovative technological advancements. Such flexibility will ensure that the statute remains relevant in the face of innovation and does not need to be amended every time a new technology emerges.

State Attorneys General and state officials or agencies should also be granted the power to enforce the provisions of the law. While FTC enforcement is certainly crucial and necessary, the Commission cannot be expected to investigate and take action against all potential violations of the new data privacy rules. Attorneys General and other state officials can step in and ensure that consumers are fully protected, as they have already successfully done in other areas, such as data breach notification.

Consumers Union also believes that the legislation should include some form of a federal private right of action. Consumers should be able to enforce their data privacy rights against companies that misuse or fail to safeguard their personal information.

**RECOMMENDATION #2:** Focus on Transparency, Purpose Specification, Use Limitation, and Auditing

Consumers Union agrees with the DOC that the baseline privacy framework should include the principles of transparency, purpose specification, use limitation, and accountability. However, to focus solely, or even primarily, on these particular FIPPs is to further encourage the development of the failed notice-and-choice model. While it is definitely important for entities to be transparent about their uses of information and to specify the purposes for which information is collected, this places the burden on consumers to understand and evaluate such statements, and make meaningful decisions to protect their data. Companies should share this burden by incorporating meaningful privacy protections directly into their day to day data collection and use activities. The FTC has already articulated this “privacy by design” principle in its recent privacy report,<sup>3</sup> calling on businesses to set up internal data minimization and data retention limits, in addition to ensuring transparency, purpose specification and use limitation. Fewer privacy concerns will arise if only necessary data is collected and stored for a limited amount of time. A privacy framework that allows a company to collect an infinite amount of data and hold onto it indefinitely as long as that company is transparent about its practices would be a troubling one indeed.

**Transparency.** Transparency can be enhanced through the use of clear, concise, and streamlined privacy policies. As outlined in the DOC report, current privacy policies are often written in order to satisfy legal obligations, not to facilitate consumer understanding. The number and complexity of current privacy policies is overwhelming to the average consumer and cannot provide meaningful notice of a company’s privacy practices.

---

<sup>3</sup> Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,” Preliminary FTC Staff Report, p. 41 (Dec. 2010). [hereinafter ‘*FTC Privacy Report*’]

Consumers Union believes that a simple, streamlined privacy policy must be developed that allows consumers to easily compare and contrast companies' privacy practices. These streamlined privacy policies could be industry-specific and could be developed through a collaboration of stakeholders representing industry, consumer groups, and government. Such privacy policies should use clear, simple language and sentence structures, and use an easy-to-read format like bullet points or charts. The privacy policies should be as concise as possible, allowing consumers to quickly scan them and understand the most important pieces of information. The privacy policy could certainly include links to more detailed discussions and explanations of individual sections of the policy, but the main page should be geared towards helping the consumer understand how the company will be collecting and using his or her data, not towards fulfilling legal requirements. Finally, the privacy policy should be easily accessible and readily available to the consumer *before* the consumer has to reveal any information to the site.

Transparency will also be promoted if the links to the privacy policies are placed prominently on the website and not hidden at the bottom of the page in tiny, inconspicuous print. This could possibly be achieved by creating a uniform button that can be prominently placed on all sites where commercial data is collected.

Transparency-enhancing techniques need to be adapted to fit the different forms of media from which websites can be accessed. Different media include computer screens, tablet screens, and mobile phone screens. A privacy policy for a given site thus should be modified in terms of presentation depending on whether it is accessed from a computer or a mobile phone.

CU supports the concept of privacy impact assessments (PIAs) because such assessments would force companies to evaluate their own practices and discover any potential privacy risks. PIAs should focus on evaluating new technology uses versus the privacy risks involved. They should be updated every time a new process of data collection is used by a company. Although we do not foresee PIAs as being an important source of direct information for consumers, they may prove helpful to government entities and non-governmental organizations wishing to evaluate an entity's privacy practices.

**Purpose specification and use limitation.** CU certainly agrees that companies must disclose the purpose for which personal information is collected, as well as refrain from using that information for any other purpose not expressly approved by the consumer. These principles, diligently implemented, will enhance trust by showing consumers that companies will behave as expected, and not another way.

In order to be truly meaningful, however, these two FIPPs must be coupled with substantive rules, set in place by legislation and rulemaking, that would require data minimization standards and data retention limits. As previously mentioned, in the absence of such substantive requirements, the notice-and-choice model would remain the primary tool for protecting consumer privacy. Companies could engage in egregious data collection and use practices as long as they informed consumers that they were doing so. Because consumers often do not read privacy policies, they would unwittingly be agreeing to the egregious practices without realizing how their personal information would be used and shared.

**RECOMMENDATION #3: Dynamic Privacy Protections through Voluntary,  
Enforceable, FTC-Approved Codes of Conduct**

Consumers Union has some concerns regarding DOC's focus on voluntary, enforceable codes of conduct as the key to implementing a FIPPs-based framework. Industry self-regulation initiatives in the past have not proven successful in protecting consumer privacy online, and have done little to nothing to restore consumer confidence in online data collection and use. As a result, we are hesitant to endorse such industry self-regulatory initiatives as the centerpiece of a future data privacy framework.

However, we do understand that advances in technology occur extremely quickly, almost on a daily basis, and that even when granted flexibility to adapt legislation to new practices, the FTC may not be able to act quickly enough to address all emerging technologies. As a result, if voluntary codes are to be developed, they must be equally as, or more, protective of consumer privacy when compared to existing legislation or rulemaking. Such codes must, first of all, be firmly rooted in some baseline, comprehensive privacy legislation. Secondly, such codes must be evaluated by the FTC and approved only if they are truly robust and provide equal or greater privacy protections than the existing framework. Third, such codes must be enforceable by the FTC, and should be evaluated on a constant basis to ensure they are still relevant and appropriate. Fourth, these codes must be developed in addition to FTC rulemaking, not instead of it. The FTC should be given the authority to interpret and implement the law through

rulemaking; any entity not willing to participate in the voluntary codes must be subject to the provisions of the statute and FTC rulemaking.

The voluntary, enforceable codes could be developed through the collaboration of industry stakeholders, government, and consumer advocates. By leading a multi-stakeholder convening, the DOC, working through the proposed Privacy Policy Office, could encourage the development of innovative privacy initiatives, such as the “Do Not Track” mechanism proposed in the recent FTC privacy report.<sup>4</sup> Stakeholder meetings of this kind, however, must take consumers’ interests into consideration in a meaningful way. Consumer and privacy advocacy organizations should be adequately represented at any such convening. This would be the only way to ensure that consumers’ voices are being heard.

**RECOMMENDATION #5: FTC as the Lead Consumer Privacy Enforcement**

Agency for the U.S. Government

The Fair Information Practice Principles (FIPPs) should be incorporated in a baseline privacy framework, adopted through legislation and implemented through FTC rulemaking. The statute should grant the FTC broad rulemaking powers to implement the FIPPs and to enforce the provisions of the statute and regulations. FIPPs should be investigated under the “unfair and deceptive” jurisdiction of Section 5 of the Federal Trade Commission Act, with reliance on the FIPPs.

---

<sup>4</sup> FTC Privacy Report, p. 63.

Voluntary, enforceable codes of conduct, if necessary, should be implemented only after the FTC has concluded a full review and granted an ex ante “seal of approval.” Alternatively, should the FTC determine such prior approval would be difficult to effectuate prior to full implementation of the program, we would also support the FTC delaying its approval until the code has been in use for a specific amount of time and has demonstrated its utility.

**RECOMMENDATION #7: Comprehensive Data Security Breach Framework**

Almost every day, new data breach incidents lead to identity theft, lost revenue, and decreased consumer confidence in the way their personal information is handled in the marketplace. The incidents often occur through inadvertent disclosures, physical loss of stored paper or electronic records, data theft by company insiders, and data breach by third parties through hacking or malware. Sometimes, these incidents affect ten or twenty consumers. Other times, the private information of hundreds of millions of Americans is compromised.

In order to address this issue, CU supports the adoption of a comprehensive commercial data security breach framework that would apply both to online and offline records. CU hopes that a robust bill would include notification provisions, strict data security protocols and requirements that entities responsible for a data breach provide periodic credit reports or pay for a security freeze in order to protect consumers from harm.

Legislation should not include a risk threshold in order to trigger the notice obligation. If necessary, the legislation could include an exemption for documented instances of breaches that pose no significant risk. Through the threshold approach, entities would not come under the requirements of the law unless there is some risk (reasonable or significant) that the information could be used to commit identity theft or harm the consumer. This particular framing is problematic because companies could simply say they do not know if the data breach presents any risk of identity theft, thus avoiding the law's requirements. CU would prefer the exemption approach, under which all entities involved in a data breach are covered by the law's requirements, but an exemption is available for entities that determine the data breach presents no significant risk of identity theft or harm. As a result, a company could not easily escape the requirements of the law by simply claiming they do not know whether a risk exists or not. Any risk determinations by the company must be submitted to the FTC.

CU also supports providing periodic free credit reports or payment of security freeze fees to consumers whose personal data has been involved in a security breach. Consumers should not have to bear the costs of securing personal information when a data breach is caused by a company's inadequate data security practices.

State Attorneys General should have enforcement authority over the provisions of the bill. In addition, CU prefers that the federal law set a floor rather than a ceiling, allowing states to implement more robust security requirements to protect their consumers. If such an approach is not possible, however, we hope that any pre-emption included in the bill will be narrowly tailored to strike out only state laws on the same exact subject matter as the bill.

CU believes that a national standard would provide industry with clear guidelines regarding the proper way to safeguard consumer data, as well as actions to take in case of a breach. This bill could also have the added effect of inducing companies to impose data minimization processes and data retention limits, in order to ensure that they are not collecting more data than they absolutely need.

**RECOMMENDATION #8: A Baseline Commercial Data Privacy Framework Should Not Conflict with Already-Existing Sectoral Laws and Policies**

Consumers Union agrees with DOC that any baseline data privacy framework should leave in place existing sectoral laws. Many sectoral laws currently in place and which have provided valuable consumer protections for privacy and data protection do not extend across all industries. In addition, certain groups of Internet users, such as children, need additional online privacy protections that would be inappropriate for the rest of the population. As a result, CU hopes that any new comprehensive data privacy law will work in conjunction with existing sectoral laws.

CU would like express some concern, however, that the DOC privacy report makes no mention of the need for heightened privacy protections for teens using the Internet. Teens between the ages of 13 and 17 make up a large portion of Internet users today. At the same time, they are more vulnerable to inappropriate uses of their personal information online, especially

because many of them do not understand the potentially detrimental consequences of freely sharing personal information. Congress has already addressed the privacy of children under the age of 13 by passing the Children's Online Privacy Protection Act (COPPA), which seeks to place parents in control over the type of information collected from their young children online. We hope the DOC will support heightened protections for teen users as well. Sites aimed at adolescents, for example, should provide greater controls, transparency, and limits on information collection. DOC should require that Privacy Impact Assessments (PIAs) detail what protections companies are offering to adolescents, and to spell out if they offer none.

**RECOMMENDATION #9: State Law Preemption**

Any baseline privacy legislation should represent a floor, not a ceiling, in terms of setting the national standard for online privacy and data security. States should be permitted to act as “laboratories of democracy,” implementing innovative means to protect consumers’ privacy online. In addition, State legislatures are often better positioned to act quickly to respond to consumers’ concerns, as well as to newly-emerging technological advances.

However, should state law preemption become part of the framework, it must be narrowly tailored to include only laws addressing the same exact subject matter found in the federal law. In addition, states should be permitted to continue enforcing their own deceptive and

unfair practices statutes and state Attorneys General should have enforcement power over the Federal law.

## **CONCLUSION**

Consumers Union commends the DOC for its interest in finding a balanced framework that would address consumer privacy concerns, as well as streamline privacy practices for business. Consumers Union agrees with the DOC that the growth and development of the Internet as a powerful political, economic, educational, and cultural tool depends to a great degree on the amount of confidence consumers have that their personal information will be responsibly used. In order to enhance consumer trust and create certainty and clarity for business, we believe that any initiative to set in place standardized privacy protections must begin with robust, FIPPs-based legislation, implemented and enforced by the FTC.

The adoption of a “privacy by design” principle, as outlined in the FTC report, will be the key to the success of this piece of privacy legislation. For too long, consumers have carried the entire burden of online data privacy by being forced to read and understand complex privacy policies drafted more with an eye towards legal compliance than consumer understanding. Requiring companies to incorporate substantive privacy practices into their day-to-day activities will hopefully redistribute that burden, so that it is shared by both companies and consumers. In addition, granting consumers a simple, persistent means to protect their privacy, such as a proposed “Do Not Track” mechanism, could go a long way toward ensuring consumers have meaningful participation in the way their information is used online, thus enhancing consumer

trust. Combined, the above-mentioned factors and recommendations will help protect consumer privacy and increase consumer confidence in the Internet, while also giving businesses clear guidelines, so that they can grow and innovate with confidence.

Thank you for the opportunity to comment on this important initiative, and we hope to work with you in the future in order to support and implement the proposals discussed.

Sincerely,



Ioana Rusu  
Regulatory Counsel  
[irusu@consumer.org](mailto:irusu@consumer.org)



Michelle Schaefer  
Esther Peterson Fellow  
[schami@consumer.org](mailto:schami@consumer.org)

Consumers Union – Washington, D.C. Office  
1101 17<sup>th</sup> Street, N.W.  
Suite 500  
Washington, D.C. 20036  
Tel: (202) 462-6262  
Fax: (202) 265-9548