Before the
U.S. Department of Commerce

In the Matter of the Request for Comments on the Department of Commerce's Report Entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework"	**)** **)** **)** **)** **)** **)** **)** **)** **)** **)**	**Docket No. 01214614–0614–01**

COMMENTS

OF THE

INTERNET COMMERCE COALITION

Jim Halpert
Callie Carr

DLA Piper
500 Eighth Street, NW
Washington, DC 20004
(202) 799-4000

January 28, 2011

January 28, 2011

FILED ELECTRONICALLY

National Telecommunications and Information Administration
US Department of Commerce

In the Matter of the Request for Comments on
Department of Commerce's Report Commerce's Report
Entitled "Commercial Data Privacy and Innovation in the
Internet Economy: A Dynamic Policy Framework"
Docket No. 01214614–0614–01

Comments of the Internet Commerce Coalition

The Internet Commerce Coalition ("ICC"), a coalition of leading Internet service providers and e-commerce companies and trade associations, is pleased to respond to the U.S. Department of Commerce Internet Policy Task Force's "Green Paper" on privacy: "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" ("Green Paper").

ICC members are key providers of e-commerce, online and telecom services, such as AOL, Amazon.com, AT&T, Comcast, eBay, Inc., Monster.com, Time Warner Cable, Verizon, TechAmerica, and USTelecom. Our diverse members represent important sources of American jobs and generate substantial economic activity involving large and small business alike.[1] ICC members devote significant efforts and resources to protecting the privacy of their customers, implement "privacy by design" methods and extensive privacy and data security compliance programs.

As President Obama emphasized in his State of the Union Address, it is essential that the U.S. remain an industry leader in the technology sector, including with regard to the Internet and communications and that it increase its competitiveness internationally in technological development. This will solidify the position of the U.S. as a global leader in technological innovation and add high-value jobs at a time when those jobs are most needed.

We appreciate this opportunity to offer comments based on our members' extensive experience with privacy issues in the technology sector.

[1] For example, USTelecom membership alone includes many mid-size companies and hundreds of small businesses.

I. INTRODUCTION AND SUMMARY

We appreciate the thought and effort that went into the Green Paper's proposed framework, its recognition of the important role of self-regulation in the U.S. privacy framework, and its recognition of the importance of adopting a flexible framework that adapts to technological change and encourages innovation.

The Department of Commerce approach is constructive and interesting in that it: (1) proposes the development of voluntary codes of conduct that provide flexibility; (2) recognizes that government should act as a coordinator of the process and a backstop for entities that do not participate in self-regulatory programs, but should not set detailed requirements; (3) recognizes that prescriptive legislation may "lock-in outdated rules that would fail to protect consumers and stifle innovation;" and (4) recognizes, in the proposed FIPPs, that transparency and "accountability" tailored to protecting privacy are more appropriate than broad requirements for data access or restrictions on data retention because such restrictions may stifle technological development and will not necessarily lead to greater consumer understanding of privacy practices.

In addition to affirming these conclusions, we urge that the Final Report embrace two other principles that are important to both innovation and protection of personal privacy. First, that it explicitly recognize the difference between use and disclosure of anonymized or aggregated data, as opposed to personally identifiable information, and between first party/affiliate usage of personally identifying information and disclosures to unaffiliated third parties. Second, that it specifically embrace the principle of technology and competitive neutrality with regard to data usage and disclosure practices and methods of securing personal data.

Furthermore, the Green Paper does not adequately address significant contradictions and confusion in the U.S. federal and state privacy framework, is too reticent about preemption, and, without several critical modifications, would actually create more of the uncertainty that it rightly decries.

The ICC is very interested in working with the Department of Commerce on enhancements to the U.S. privacy framework that would create baseline privacy protections, provided that the enhanced framework:

(1) establishes uniform, cross-industry, national standards (there is greater integrity and transparency if the standards are cross-industry);

(2) resolves confusion for businesses and consumers caused by ambiguous, widely varying, and overlapping privacy regulation of rapidly converging communications services; and

(3) provides for enforcement by self-regulatory organizations, the Federal Trade Commission ("FTC"), and state attorneys general, while precluding private rights of action for statutory damages (including attorney general outsourcing of enforcement to the plaintiff's bar).

We agree that there may be room for an overarching system based on very strong notions of transparency, predictability and consumer choice and control (standardized short notices, for example, would be a very positive development). However, the Department of Commerce should take very seriously its pledge of flexibility so that the framework can evolve with continued rapid technological change.

II. KEY POINTS IN THE FRAMEWORK AND QUESTIONS

A. *Resolving Ambiguity in Overlapping Privacy Regulation*

The rapidly converging communications services industry is currently regulated under widely varying, highly complex rules that apply through Consumer Proprietary Network Information regulations, the Cable Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, state recording statutes, and state online and Internet service provider privacy laws.

At least as applicable to the communications sector, we disagree with the assumption in the Green Paper that all existing sectoral regulation should be preserved and that the new framework should apply alongside or in addition to this already complex and confusing body of regulation. This would lead to further confusion, uncertainty, and regulatory costs and barriers to innovation in the U.S. communications sector.

B. Providing Enforcement by Self-Regulatory Organizations, the FTC, and State Attorneys General – No Private Right of Action

We support enforcement through self- regulatory organizations, the FTC, and state attorneys general, while precluding private rights of action, including attorney general outsourcing of enforcement to the plaintiff's bar.

Private lawsuits are extremely inefficient and enrich plaintiffs' lawyers without significantly benefiting consumers. Proposals, such as those found in the Rush privacy bill introduced in 2010 and Senator Kerry's draft privacy bill, for a private right of action for statutory or treble damages for "willful" violations and attorney fee shifting are in no way a viable compromise on this issue (intent is a jury question). This standard would attract nuisance lawsuits claiming huge statutory damages that consume significant litigation expense.

There are ample alternative incentives to induce companies to participate in self-regulatory programs without this wasteful tool. Similarly, proposals for civil penalties of up to $5 million for garden-variety privacy or data security violations without any requirement for harm to consumers are disproportionate.

Company privacy commitments voluntarily adopted through self-regulatory regimes are better enforced under the FTC's existing unfair and deceptive trade practice authority, which generally functions very effectively to deter violations by companies. In addition, we believe that enforcement and "public shaming" by non-governmental, self-regulatory organizations, such

as Truste, BBBOnline and CARU, can be an effective complement to government enforcement by referring cases for government enforcement or publicly criticizing company practices.

C. *FTC Role*

As discussed below, FIPPs could be a promising approach to transparency and accountability. The appropriate implementation of a broad-based FIPPs framework should be developed by relevant industries, who best understand the intricacies of implementing such a program. Such a framework should be, to the extent practicable, a voluntary, self-regulatory framework, rather than inflexible binding rules that would be implemented if the FTC were given rule-making authority. However, the FTC should have Section 5 authority, and self-regulatory authorities should also have the authority, to enforce the failure of actors to follow the general FIPPs or to adhere to a similar self-regulatory framework.

D. *Fair Information Practice Principles (FIPPs)*

The FIPPs detailed in the Green Paper are a potentially promising approach to achieve transparency and accountability, if they provide flexibility and allow for the development of tailored implementation through industry self-regulation and do not create a regulatory framework.

That said, it is important that any such FIPPs be neutral – for example there is no evidence that consumers regard "cookie-based" tracking as any less problematic or invasive than tracking that relies upon deep packet inspection that retains a similar amount of data.

In addition, the full range of FIPPs, which are appropriate for the Department of Homeland Security's use of personal information, are clearly inappropriate for non-sensitive data and for the overbroad range of "consumer data" such as that found in the FTC Staff Report's[2] definition of "consumer information." Rather, several factors should bear on the array of FIPPs that should apply in any particular context: (1) the type of data (financial, medical, children's, etc.); (2) the form the data are in (personally identifying, not combined with information that identifies an individual, permanently de-identified, aggregated); and (3) the purposes for which data are used or disclosed (for example, whether the data are disclosed to third parties for profiling, used to deny credit or employment, used by a first-party).

We submit that the core privacy issue of the information age is the compilation of personally identifying profiles about consumers by third-party entities with which consumers have no relationship and no understanding. Much broader FIPPs are appropriate for this "information proliferating" activity than for first-party uses, or clearly disclosed uses by affiliates of a first party..

[2] Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010).

E. *Notice and Choice*

Notice and choice does not address all privacy issues, but it does remain a viable model for addressing many aspects of consumer privacy, provided that notice is transparent. Of course, consumers must understand the choices they have regarding privacy, but if notice is transparent, then notice and choice should continue to be an option for resolving issues such as material changes in privacy practices.

F. *Audits*

Audits have an important role to play as part of internal privacy compliance as a way to measure compliance and fix problems. However, they can be very expensive and are not a valid basis for enforcement actions under the existing FTC framework, which has no clear scienter requirements, and requiring publication of audit results would be both inappropriate and counterproductive.

First, organizations, particularly in the Internet environment, are dynamic. Acquisitions of business units, creations of new business units, and reorganizations of existing business units are frequent. As a result, business units are adding and subtracting new business units to their compliance structures frequently. It would be a major burden on innovation to create significant compliance risks for those changes as business units transition to different compliance mechanisms.

Second, the integrity of audits will inevitably be compromised if reports trigger enforcement actions or private lawsuits. Enforcement should follow only after repeated, willful, and material failures to comply. For both reasons, auditing, while a very useful compliance tool, is better used to measure compliance and then fix compliance issues.

On the other hand, self-regulatory organizations and the FTC should have the ability to audit participating companies for compliance.

G. *Privacy by Design v. Privacy Impact Assessments*

We strongly endorse and our members practice “Privacy by Design reviews” of new services and new uses or disclosures of personal information for consistency with companies’ privacy statements and guiding principles. The communications industry, for example, has long considered privacy concerns in the product design stage. All our members also implement accountable business practices and robust security measures, assign personnel to oversee privacy issues from the earliest stages of development and train employees on privacy.

By contrast, the Department of Commerce should refrain from a full-fledged endorsement of privacy impact assessments to the extent that they are broader than reviews of new products, new services, and new uses or disclosures of personal information. Privacy impact assessments appropriate for the Department of Homeland Security are not appropriate across the technology sector or other broad commercial sector, as recent debates about airport scanning equipment exemplify. Indeed, if they were applied in the commercial sector to the

broad range of consumer data discussed n the FTC Staff Report and several congressional privacy bills, they would be very lengthy and complex, and would defeat the transparency interests that they are intended to further.

On the other hand, Privacy by Design is a valuable addition to the FIPPs.

H. *Purpose Specification and Limitations of Use Categories*

The Green Paper's suggestion of "purpose specification" and "limitation of use" categories as elements of notice and alternatives to data minimization and destruction mandates is an interesting, constructive, and positive basis for further reflection. That said, in order to achieve transparency, it is important that such categories not be prescriptive. Industries know that transparency is important, and they have every incentive to make sure consumer notices are clear and understandable. However, strict rules regarding notice requirements could lead to even longer, more complex privacy statements that are difficult to understand and thus defeat the goal of transparency.

It is equally important to recognize that the critical goal of transparency can be achieved only through general purpose specifications. This requires an important change/clarification to the FTC's enforcement of its *Gateway Learning* "material changes" principle, which currently drives companies to exhaustive disclosures of all possible uses and disclosures of personal information. The broad, opt-in requirement interpretation of *Gateway Learning* would unfortunately be codified in several federal privacy bills and draft privacy bills circulated over the past year.

A better approach would be to encourage *general* purpose specifications and use limitations that cover potential uses in fewer words and clearer terms. If these are incomplete and a business proposes to make a materially privacy-reducing use or disclosure of personal data, they should be required to provide concise, transparent notice and offer consumers a clear choice about the use or disclosure.

I. *PII v. Non-PII*

It is important for U.S. innovation and for privacy protection that the Final Paper recognizes a significant distinction between information that is identifiable at an individual level and information that might be made identifying, but is not. The key test is not whether information might be made identifiable, but whether it *is identifiable to an individual level.*

By treating all IP addresses and all numbers linked to any other device as equivalent to personal data, as the FTC Staff Report proposes, the framework would actually eliminate incentives to hold data in non-identified form and limit innovation. IP addresses and device identifying numbers are routinely used on the Internet for a host of important purposes (for security, spam prevention, recognizing a return user, etc.), and are routinely collected by the way the Internet operates. An expanded FIPPs framework is more costly and should not waste compliance resources on information that is not personally identifying and as to which a purpose

specification states that it will not be used in identifying form.

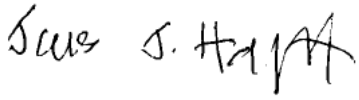
Exceptions should apply where: (1) the non-personally identifying data are combined with other data that makes the person identifying, and thus are no longer non-identifiable; (2) an IP address or other identifying number is used by a third party with whom a consumer has no relationship in a profile that will be disclosed to others, or (3) the information is made publicly available (and thus exposed to hackers who can attempt to derive the identity of the user). However, there should be narrow exceptions to the presumption that consumer data subject to the FIPPs framework is data that identifies an individual. Other than that, IP addresses and similar device-related data or information that has been de-identified should not be subject to the framework, except that companies should, of course, be held to any purpose specifications with regard to keeping data non-identifying and should bind third parties who receive such information to keep it only in non-identifying form.

J. *Privacy Policy Office ("PPO")*

The PPO position could be a constructive way to encourage the participation of more businesses in the development and implementation of more self-regulatory programs. It is important that the industry, which is best suited to understand the challenges of implementing any such programs, suggest the content of the self-regulatory guidelines. However, the PPO can be very helpful in encouraging more businesses to participate and in suggesting ways to make self-regulatory codes more consistent in their approach to issues, such as transparency, where similar approaches are desirable.

We thank you for considering our views, and are eager to continue to work with the Task Force in a constructive fashion to help achieve the Department of Commerce's goals of balancing consumer transparency and choice with beneficial uses of information and continued technological innovation.

Sincerely,



Jim Halpert, General Counsel
Callie Carr, Counsel