Before the
Federal Trade Commission

In the Matter of the Request for Comments on the Preliminary Federal Trade Commission Staff Report: "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"	)	**File No. P095416**

COMMENTS

OF

THE INTERNET COMMERCE COALITION

Jim Halpert
Callie Carr

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

February 18, 2011

February 18, 2011

FILED ELECTRONICALLY

Federal Trade Commission
Bureau of Consumer Protection

In the Matter of the Request for Comments on the Preliminary Federal Trade Commission Staff Report: "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"
File No. P095416

Comments of the Internet Commerce Coalition

I. INTRODUCTION

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 Federal Trade Commission's ("FTC") Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" ("Staff Report").

ICC members are key providers of e-commerce, online, and broadband access services: AOL, Amazon.com, AT&T, CareerBuilder, 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. ICC members devote significant efforts and resources to protect the privacy of their customers and implement "privacy by design" methods and extensive privacy and data security compliance programs.[1]

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 the U.S. increases its international competitiveness in technological development and innovation. This will solidify the position of the U.S. as a global leader and facilitate the creation of high-value domestic jobs during these challenging economic times.

Much of the Staff Report is directed at perceived challenges that technology poses to personal privacy. It is critical that the Commission's final privacy framework avoid hindering technology innovation and that it strike the right balance between the important objectives – privacy protection and economic growth.

[1] Please note that these comments do not necessarily reflect the views of all of the ICC's members.

II. SUMMARY

We appreciate the thought and effort that went into the Staff Report's proposed framework, and the recognition that the Staff Report extends to, and the role it allows for, self-regulatory industry initiatives.

We agree strongly that transparency and predictability of data practices should be improved, that consumer opt-out choices could be simplified and made more user friendly (without a "Do Not Track" mechanism), and that best practices relating to data governance, which the Staff Report groups under the category "Privacy by Design," should be more widespread.

The communications industry generally and all ICC members in particular have successfully implemented the features of the Staff Report's "Privacy by Design" ideas well before they were known as "Privacy by Design." The features of "Privacy by Design" that the ICC members have successfully implemented include internal data governance/management structures to protect consumer data, measures to ensure proper use of personal information, privacy considerations in the product design stage, accountable business practices and robust security measures, privacy personnel involvement in the earliest stages of development, and employee training in privacy rules and regulations. The ICC supports adoption of these principles as part of an expanded best practices framework.

We also appreciate the Staff Report's recognition that a clear, simple, and prominent opt-out mechanism may be more privacy protective than a confusing opt-in provision or many opt-out notices. Creating a regime where routine activities such as opening a web page or clicking on a link could result in a barrage of notices would unnecessarily impede consumers' online experiences. It takes time and effort for consumers to understand even simply stated options for informed consent. Accordingly, consent requirements should be reserved for decisions that matter to consumers. Requiring notice and choice for a broad range of activities would dilute the efficacy of notices, and it would negate efforts being made by Internet businesses to simplify privacy notices and choices for consumers.

At the same time, we believe that the Staff Report does not address significant contradictions and confusion in the U.S. federal and state privacy framework and would have the effect of exacerbating these contradictions and confusions unless it supersedes some current regulatory requirements.

In addition, we have several other specific concerns with respect to the proposed framework:

(1) The Staff Report's assumption that IP addresses and device identifying numbers should, in most or all circumstances, be considered personal information would create serious obstacles to important Internet functionalities (such as delivering a web page, providing security, delivering personalized content, and identifying a user's ISP). In addition, equating IP addresses and device identifying numbers with personal information would have the perverse effect of eliminating current incentives not to identify

technology users and to limit the collection and use of information that truly identifies people, such as name, address, telephone number, account numbers, social security numbers, and email addresses.

(2) The Fair Information Practice Principles ("FIPPs") described in the Staff Report must be more flexible than suggested by the Staff Report, so that the FIPPs can adapt to rapid changes in technology. For example, while a category of exempt, expected, or industry-standard uses is an important feature of an enhanced privacy framework (to avoid long privacy notices consumers will not read), the category of "commonly accepted practices" is subjective and inherently under-inclusive. In addition, given the expense of implementing the full range of FIPPs, we believe that the application of FIPPs should be adjusted based on the particular context, including the type of data in question (e.g., sensitive or non-sensitive), the form the data are in (e.g., personally identifying or not personally identifying), and the purposes for which the data are used or disclosed.

(3) The Staff Report's assumption that self-regulation has failed is overly pessimistic. Since the Staff Report was released, there have been at least three major, private sector self-regulatory or technology initiatives announced. While we are sympathetic to the notion that the notice and choice regime should be expanded to provide more effective ways to allow consumers to control how they are tracked, we think that there are now good self-regulatory programs in place and that the market is beginning to produce very positive alternatives as the FTC has urged. Because there are so many initiatives in this area, we think it is premature for the FTC to reject these alternatives and instead embrace any one-size-fits-all solution, such as a mandatory "Do Not Track" mechanism.

We support the Department of Commerce Green Paper's ("Green Paper") approach to a revised framework[2] because it proposes the development of voluntary codes of conduct that provide flexibility and 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 that government should not set detailed requirements. Furthermore, it recognizes that prescriptive legislation may "lock-in outdated rules that would fail to protect consumers and stifle innovation."[3]

(4) We believe that any proposed framework should be scrupulously technology neutral, just as the FTC's Privacy Principles in its 2000 Report to Congress tried to be technology-neutral.[4] Favoring a particular technology solution for "Do Not Track" would be a sharp and unjustified departure from the FTC's record of technology neutrality in Internet policy. The important consideration is how the data is used, not the technology collecting the data.

(5) Many of the questions in the Staff Report open the door to adding far greater complexity to any proposed framework (for example defining retention periods, adding a

[2] Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 16, 2010) at 5; part II(C)(1).
[3] *Id*. at 5; 29; part II(C)(1); part II(C)(3).
[4] Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress (May 2000) at iii.

broad set of access and correction rights, etc.). We submit that an elaborate framework would increase the costs of compliance and greatly reduce adoption of such a framework.

III. KEY POINTS IN THE FRAMEWORK AND QUESTIONS

A. *Generally*

The ICC is very interested in working with policymakers on enhancements to the U.S. privacy framework, provided that the enhanced framework is self regulatory, and

(1) establishes uniform, cross-industry, national, self-regulatory 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;[5] and

(3) provides for enforcement by self-regulatory organizations, the 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). Such actions are extremely inefficient and enrich plaintiffs' lawyers without significantly benefiting consumers (private rights of action are incompatible with even very strict privacy regimes, such as the privacy regime in the European Union).

We agree that there may be room for adjustments to the current privacy framework based on very strong notions of transparency and predictability and consumer choice and control. We are interested in exploring standardized, short privacy notices as a way to promote transparency, for example. However, the FTC must allow for flexibility so that the framework can evolve with continued rapid technological change.

B. *Specific Elements of the Framework*

1. IP Address and Personally Identifiable Information ("PII").

The Staff Report's proposed standard of including IP addresses and information that identifies a device as PII is unworkable and inconsistent with the many existing privacy laws where a clear PII/non-PII line has been drawn. There is also insufficient support in the record for such an approach. The key test is not whether information might conceivably be made identifiable, but whether it *is identifiable to an individual level.*

[5] These are currently regulated under widely varying, highly complex rules that apply through Consumer Proprietary Network Information rules, the Cable Act, the Video Privacy Protection Act, state recording statutes, and state online and ISP privacy laws. At least as applies to the communications/technology sector, we disagree strongly with the assumption in the Staff Report 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 communications sector.

An IP address is not factually identifiable to an individual level. An IP address may be able to be associated with a particular "household user" through subsequent matching searches/browsing, but the individual is not identifiable through the IP address itself. Rather, other data sources would have to be combined with an IP address to make a person individually identifiable. The fact that an IP address or other non-identifying data might be personally identifiable in one case out of tens or hundreds of thousands, or might be identifiable if publicly disclosed and analyzed by computer scientists, when that has not in fact occurred, in no way justifies treating all such information as subject to the privacy framework requirements.

By treating all IP addresses and all numbers linked to any other device as equivalent to PII, the framework would actually eliminate incentives to limit the collection of information, including PII, and to hold data in non-identified form. This decision would likewise limit innovation. In addition, the framework would be impracticable because IP addresses must be used for several important functions. For example, IP addresses must be logged to deliver a web page, for security purposes (including to protect against spam), to deliver personalized content to a user, to inform consumers of information they have previously viewed on a webpage, and to identify a user's ISP.

IP addresses can also provide other information about a consumer that allows the consumer to receive beneficial information. For example, an IP address can be used to direct a consumer to local news and weather updates (including local area alerts – blizzard, tornado, hurricane, flood), to help the consumer find the closest gas station, restaurant, store, ATM, parking garage, etc, to provide the consumer with turn-by-turn directions based on the consumer's current location, or to deliver relevant local advertising to a consumer.

That said, we do understand that special requirements might apply where an IP address is used to build a pattern of web surfing behavior by a third party with whom a consumer does not have a relationship.

In response to the Staff Report's questions under the "Scope" category with respect to IP addresses and PII, we do not believe that the "can reasonably be linked" or "reasonably linkable in the future" standards are workable, as this varies widely depending upon context. For example, if information is made publicly available and is subject to attacks from hackers or tinkerers trying to identify individuals, the information may be linkable. However, if it is never made publicly available or is not hacked, and is not combined with information that is identifying, then it will never be linked. Accordingly, we believe that if information is kept in a secure database and is never linked by the person holding the data, then the data should not be subject to the framework. It is equally true that where information in theory can be identified in the future, but the risk of that occurring in the future is very small, it should not be subject to the framework unless such linking occurred at some time in the future.

In any event, the final Staff Report should clarify that methods of de-identifying data so that it cannot be identified by the recipient, including but not limited to single hashing, double-hashing, encrypting and data aggregation, exempt such data from the framework, provided that the protection is not removed. This clarification would encourage strong data protection

practices and innovation in de-identification technologies.

2. "Commonly Accepted Practices"/"Reasonably Anticipated Practices" and First-Party Marketing.

We commend the FTC for recognizing that there are a host of activities that people expect or should expect are occurring (for example, where they enter address information on a website for order fulfillment or where the information is used for fraud prevention or legal compliance).

That said, we do not believe that the term "commonly accepted practices" is the correct term to use. This term is circular and incorrectly implies that no other activities are "commonly accepted". The phrase "reasonably anticipated" may be a more appropriate term.

Likewise, a specific list of reasonably anticipated practices would be far too subjective and would cause too much and irrelevant information or too little relevant information in privacy notices, which is counterproductive to the framework's goals. Instead we believe that a set of broad, general principles, should be developed that are flexible enough to account for specific circumstances and technology and to encourage innovation.

In fact, there are several very important first-party (and third party agent or service provider) uses of data. For example, service delivery, billing, analytics, infrastructure planning, or future product development are all important uses of consumer data that are standard functions in improving services and that should be expected by consumers. Excluding them from exempt practices would cause economic harm without materially improving privacy.

In addition, it is critical that any list of reasonably anticipated practices provide for use of information in connection with first-party marketing and market research and should account for free websites, which depend upon advertising revenue to support free content. Uses of information for first-party marketing should include affiliate sharing to the extent an affiliate is not further disclosing the information to unrelated third parties. In addition, affiliates should not be defined to include only entities that share a common brand, as brands that are advertised together by a company are commonly understood by consumers to be part of the same corporate family. An alternate rule focusing on whether the affiliates' brands are the same would artificially distort branding practices in a way that is unnecessary if companies advertise brands together as part of a family of brands.

Although we strongly believe that it is essential to preserve first-party marketing as a reasonably anticipated practice, we understand that first-party marketing might not be appropriate in every circumstance and some reasonable limitations are appropriate. Whether such marketing is appropriate would depend on the entity collecting the information, whether the information is sensitive, and the consumer's expectations for use of that data. For example, the majority of consumers would probably not be surprised if they received first-party marketing from shopping.com after purchasing a pair of shoes from the website. However, most consumers would probably be concerned after receiving first-party marketing from a healthcare portal which would have access to their sensitive healthcare information.

In response to the Staff Report's questions regarding first-party marketing we believe:

(a) First-party marketing should not be limited to the medium through which a consumer provided the information. Consumers expect that if they provide information via one medium, that information may be used to contact them via a different medium. In addition, consumers already have rights to opt-out of commercial email, fax, and telemarketing solicitations, and these are more than adequate to protect consumers in the context of first-party relationships where the consumer can take his or her business elsewhere.

(b) Financial data, other than financial account numbers, is not sensitive and should not be subject to first-party marketing restrictions. Consumers know that they are providing this information and expect that it will be used for marketing. Indeed, the Gramm-Leach-Bliley Act does not treat financial data as subject to any first-party marketing restrictions. Given that financial institutions, which hold more of such data, are not subject to these restrictions, such a rule would make little sense for non-financial institutions.

3. Accumulation of Profiles and Data Enhancement.

The proposed framework's focus on and concern about the accumulation of profiles held by third parties whom consumers have no relationship with fails to distinguish between practices that are entirely appropriate and indeed necessary to the Internet ecosystem and practices that are genuinely troubling. For example, data should be allowed to be appended to other information by a first party which has a direct relationship with the consumer if it is received from a legitimate source.

Any notification obligations with respect to data provided to third parties should fall on the party who originally collected or compiled the data and not on the party that acquired and used it. To the extent a party is required to provide notice and choice, such notice and choice should be a basic notice and opt-out required for other routine uses and not a more robust notice and opt-out.

Similarly, first-party companies should be required to provide transparency about data enhancement practices but should not be subject to consumer choice unless the first-party company shares consumer data with the entity providing the data enhancement. There are many business reasons for a company needing to enhance their databases from other sources, separate from reasons associated with marketing. For example, a company may use data enhancement for security reasons and for fraud detection and prevention. Furthermore, data enhancement practices in the case of first-party marketing should be considered an acceptable practice, if handled in a responsible manner. If data is licensed appropriately and is acquired legally, then it should be treated no differently from other data.

4. Self-Regulation.

The FTC should continue to promote self-regulation, rather than seeking authority to implement or attempting to implementing formal regulations. This would be counterproductive and premature at this juncture given recent self-regulatory initiatives and the many new features of the proposed framework.

We support flexible guidelines, rather than rigid requirements, as such guidelines can better achieve the goals of encouraging innovation and protecting privacy. This approach is inline with the Green Paper's approach to a revised framework, which proposes the development of voluntary codes of conduct that provide flexibility and recognize 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. As the Green Paper noted, prescriptive legislation may "lock-in outdated rules that would fail to protect consumers and stifle innovation."[6]

5. Enforcement

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, which provide 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.

6. Do Not Track is Ill-Defined, and Depending on its Meaning, May Be Entirely Inappropriate.

The "Do Not Track" concept is referenced repeatedly in the Staff Report, but never fully defined. There needs to be an understanding of what "Do Not Track" actually means, including when "Do Not Track" means "Do Not Collect at All."[7] In addition, in light of recent self-regulatory initiatives, the FTC should avoid imposing a technology mandate or recommending a specific technology (and thereby giving enormous market power to that technology), especially a technology that is not yet ready and risks disrupting the business models of free websites. In addition the focus should be on how data is being used rather than on the technology that is being

[6] *See supra* note 3.
[7] Despite attempted comparisons, "Do Not Track" would be fundamentally different from "Do Not Call."

used to collect the data. The most important goal is to promote consumer control that is simple, easy, and transparent. Thus, the FTC should allow the market to continue to explore self-regulatory initiatives that balance constantly changing technology, innovation, and consumer control.

7. Notice and Choice.

We recognize that 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.[8]

8. Technology Neutrality and Enhanced Consent.

Technology is not inherently good or bad. Rather, the important consideration is how technology is used. Focusing on specific technologies as "good" (*i.e.*, cookies for data collection or browsers that implement "do not track") and other technologies as "bad" (*i.e.*, DPI for data collection) is ill-advised and will result in the government picking technology "winners" and "losers" and "winners" and "losers" in the competitive marketplace. In addition, this approach is inevitably outdated as new technologies are deployed.

Instead, it is important to look at how data are being used rather than focusing on one technology and requiring enhanced consent for that particular technology. For example, if deep packet inspection ("DPI") technology is used for a variety of essential technical functions (enhancing network security, for example) or collects the same information as a behavioral advertising network, it is not qualitatively different than other data collection methods and does not warrant "enhanced consent" or "heightened restrictions."

9. Restrictions on Data Retention.

Limitations on data retention for sensitive data that pose a real risk to consumers (such as SSNs or payment card information) are clearly justified, unless such data are retained securely. However, there should be no restriction on the length of time that the data is held in the context of first-party relationships, unless they relate to insecure retention of data that poses a risk of identity theft, fraud or other concrete harm to consumers. Retention limits may interfere with the ability to provide ongoing service, engage in planning new services, and in connection with other beneficial services. In addition, if the retention criterion is disclosed to consumers in a transparent manner, they can take their business elsewhere if dissatisfied.

[8] Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Concurring Statement of Commissioner J. Thomas Rosch (Dec. 1, 2010) at E-2 ("In short, to the extent that privacy notices have been buried, incomplete, or otherwise ineffective – and they have been – the answer is to enhance efforts to enforce the "notice" model, not to replace it with a new framework."); E-4 – E-5 ("…[b]ut the appropriate remedy for opacity is to require notices to be clear, conspicuous and effective.").

Furthermore, in response to the Staff Report's question regarding data retention, the reasons to retain consumer data vary, and in some cases retention is mandatory. Therefore, a single retention period cannot be prescribed. Indeed, the very same document must be held for different periods of time depending on the circumstances. The Green Paper rightly recognizes 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.[9] In addition, 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.[10]

10. Access.

We agree with the Staff Report that access rights entail significant costs. We believe that, in line with the framework in the Fair Credit Reporting Act, access rights should apply broadly with regard to third-party data brokers only, and should apply to first-party companies only for data which they have used to make a significant adverse decision against a consumer (rejection of credit, denial of service). In addition, in response to the Staff Report's question, we believe that if access is a requirement, companies should be able to charge a reasonable fee, as access can be costly.

11. Retroactive Material Changes in Practices.

Retroactive material change in privacy practices should operate with clear and conspicuous notice and opt-out if the prior privacy policy disclosed that such changes would operate that way. An opt-in exception to this rule should apply, as in *Gateway Learning*, if a privacy policy makes a key and unequivocal promise that a company will never share or sell personal data.

However, the Staff Reports suggestion that the FTC will apply an opt-in rule in the case of *all* retroactive material changes would be a counterproductive bridge too far. The Staff Report overlooks that a broad interpretation of the *Gateway Learning* material changes principle has been a major driver of "overlong legalistic notices." Today, out of fear that failure to mention a use or disclosure of personal or other consumer data in a privacy policy would trigger an opt-in requirement for retroactive material changes, companies include extensive laundry lists of potential uses and disclosures. The Staff Report's proposed broad codification of this principle is directly contrary to the Staff Report's laudable "short, clear, simple" goal for consumer notices.

If notices are to be shorter and clearer, the new framework cannot require opt-in consent for uses of consumer data if a notice and opt-out procedure for such uses was clearly and conspicuously disclosed in an initial privacy notice.

[9] Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 16, 2010).
[10] *Id*. at part II(B).

For the same reasons, it is important that transparency, rather than formal consumer requirements, apply to prospective changes to privacy policies.

12. Inclusion of EU-Style Concepts.

While we strongly welcome more global coordination on privacy in areas such as privacy by design, self-regulation, consumer education and enforcement, the inclusion of EU-style regulatory concepts must be considered very carefully as these originate from a different approach to privacy and may not meet the goals of the privacy framework in the U.S.

13. Privacy-Enhancing Technologies.

We support incentivizing the development and deployment of privacy-enhancing technologies, provided that no one technology is favored over other technologies. We recommend that this start with the FTC educating companies regarding the benefits of incorporating privacy-enhancing technologies in product development (i.e., in implementing "Privacy by Design") because many companies may be unaware of the technologies available. That said, the FTC should avoid promoting any one technology and should instead educate companies about all available technologies.

Sincerely,

Jim Halpert, General Counsel
Callie Carr, Counsel