Before the
Federal Trade Commission
Washington, D.C. 20580

In the Matter of	)	
	)	
Protecting Consumer Privacy in an Era	)	File No. P095416
Of Rapid Change	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

Rick Chessen
Michael S. Schooler
Loretta P. Polk
Stephanie L. Podey
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222 -2445

February 18, 2011

TABLE OF CONTENTS

Before the
Federal Trade Commission
Washington, D.C. 20580

In the Matter of	)	
	)	
Protecting Consumer Privacy in an Era Of Rapid Change	)	File No. P095416
	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA")[1] hereby submits its comments in response to the Federal Trade Commission's ("Commission") Privacy Report.[2]

INTRODUCTION AND SUMMARY

Protecting the privacy of consumer information transported over the Internet deserves the high-priority attention of all stakeholders in the emerging marketplace of online communications and commerce. Consumers are rightly concerned that the personal information they provide over the Internet may be collated, gathered, tracked and distributed in myriad ways so that far too many persons and entities will know far too much about them. Cable operators and programmers not only understand these concerns but are committed to protecting the privacy of their customers.

For cable operators, the privacy of their customers is not a new concern. Since long before they began offering broadband service, cable operators have been taking steps to protect customers of their cable television service against any undesired disclosure of their personally

---

[1] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing over $170 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 23 million customers.

[2] Fed. Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers* (rel. Dec. 2010) ("Staff Report").

identifiable information ("PII") and their purchasing and viewing decisions. Since 1984, such measures have been required by federal law. But they're also a business imperative – especially in today's competitive broadband marketplace. For all the services that cable operators now offer – video, broadband and telephone – consumers have choices. Moreover, more and more consumers are now purchasing all these services from a single provider, so that the costs of losing a customer to a competitive provider are compounded. In other words, cable operators have singularly strong incentives to meet the privacy concerns and demands of their customers.

But *how* to meet the privacy concerns and demands of consumers when they use the Internet is a much more complex task, and it involves a much larger ecosphere of entities, many of which may not have the same ongoing relationship with – and incentive to protect – consumers' privacy. Moreover, balancing those privacy needs against the uses of consumer information to support legitimate and beneficial Internet services and applications presents new and challenging issues for service providers and policymakers alike.

The Commission's Staff Report is a commendable effort to address those issues and help meet those challenges. The Staff Report provides a comprehensive analysis of the current state of privacy protection that identifies what appears to be working and what appears not to be working in ensuring that consumers' interests are protected. It proposes a new "framework" for addressing Internet privacy concerns, but it admirably refrains from concluding – or even proposing – that this new framework must be implemented by new legislation or regulation. Instead, the Commission sets forth its proposed framework as a "policy vehicle," leaving open the question whether the framework might effectively be adopted, in whole or in part, by the affected entities themselves, voluntarily or through self-regulatory mechanisms, or whether it must be mandated by the government.

At this juncture, there is strong reason to favor a self-regulatory approach. First of all, while the Internet inherently presents an array of privacy issues, those issues are ancillary to a competitive marketplace that is continuing to offer consumers valuable and exciting new services, content, and applications that were unimaginable only a few years ago. The economics and the technology of this marketplace are constantly evolving and in flux, and while these may be the best circumstances for innovation and consumer satisfaction, they are the *worst* circumstances for regulatory intervention. Regulation would constrain the flexibility of Internet entities to tailor their privacy protections to changing technologies, new services, and the evolving economics of the Internet. More importantly, regulation – even self-regulation – virtually always produces unintended consequences. But self-regulation can be quickly modified and adapted to remedy such consequences, while laws and agency rules, once codified, are not easily altered. And the cost of unintended consequences is uniquely high when they could affect the enormously successful and beneficial Internet ecosystem.

The Staff Report recognizes one of the ways that unduly restrictive or overbroad privacy requirements can have adverse consequences. Specifically, the Commission recognizes the importance of online advertising revenues to the economic underpinnings of Internet content and services. Such revenues supplement, and in many cases substitute for, fees that would otherwise have to be charged to consumers to support such content and services. Without them, the innovation, competition and constant expansion of available content and services that have been the hallmark of the Internet would be impaired. Moreover, forcing more of the Internet's costs to be borne by consumers would undermine the public policy goal of encouraging greater availability and adoption of broadband services.

One method of efficiently maximizing the availability of advertising revenues in such a highly competitive marketplace is so-called "targeted advertising" – advertising that is sent specifically to consumers who are most likely to be interested in particular products or services. Targeted advertising may implicate privacy concerns: How do advertisers identify the consumers who are most likely to be interested in their products? But, as the Commission understands, the benefits of such advertising must be balanced against such concerns in determining whether and to what extent it should be restricted.

The Staff Report includes many useful ideas and recommendations for balancing the interests at stake in developing a privacy policy framework. A pro-active policy of "privacy by design," for example, minimizes the risk of privacy breaches and concerns from the outset and should be a fundamental component of the development of new Internet products and services by all responsible Internet companies. The cable industry, as noted above, is committed to protecting the privacy of its customers and, to this end, our companies are continually engaged in efforts to develop best practices and promote consumer privacy at every stage of the development of products and services (including the development of targeted advertising policies and procedures).

The concept of "notice and choice" should also play a role in any sound privacy policy insofar as it enables individual consumers to decide, in certain cases, whether the benefits of disclosure of certain consumer information in certain circumstances override any privacy concerns. But, as the Commission suggests, the effectiveness of notice and choice can be undermined if it is implemented in a way that is confusing to – or ignored by – consumers. The Commission's proposal to simplify consumer privacy notices by removing from "notice and choice" those transfers of consumer information that are "commonly accepted practices" – or

perhaps more appropriately, those for which there is no expectation of privacy – is a step in the right direction.

So, too, is the Commission's recognition that for those practices that remain subject to notice and choice, there may be no single best way to offer such notice and choice in all circumstances. Where disclosure of consumer information can provide benefits to consumers (such as in the case of targeted advertising), notice and choice should be designed to ensure that consumers understand both those benefits *and* the privacy implications. Reflexive opting *out* where a consumer does not fully understand and take into account the *benefits* of disclosure of information is as undesirable as reflexive opting *in* where the consumer does not understand or cannot be expected to take the time to read the details of how and when such information will be disclosed. In particular, a uniform "Do Not Track" button, while providing an easy way to opt out of a privacy-related practice, could lead to just this sort of reflexive and uninformed choice, with unintended and unwanted consequences for consumers.

Figuring out how to adapt notice and choice to the vast array of different circumstances in which consumer information may be used and disclosed by Internet content, application, and service providers is precisely the sort of task best implemented through vigilant and ongoing self-regulation. It would be premature and counterproductive to attempt to codify rules that applied sensibly in all these circumstances, and the Staff Report cautiously avoids endorsing such a step.

Similar caution is warranted before the Commission accepts the suggestion in the Staff Report that the distinction between PII and information that is not personally identifiable has been blurred to the extent that it should no longer be relevant for privacy purposes. Privacy policy (as embodied, for example, in the privacy legislation applicable to cable television

operators) has until now generally recognized that the collection and disclosure of aggregate or anonymous data – which can serve wholly legitimate, beneficial, and pro-consumer purposes – does not raise the same concerns or require the same protections as the collection and disclosure of PII. The Staff Report summarily concludes, however, that the logic of this longstanding distinction no longer applies because of "changes in technology and the ability to re-identify consumers from supposedly anonymous data."[3] While there may be anecdotal evidence of such techniques, there are also ongoing changes in privacy-enhancing "anonymization" technologies that are designed to *prevent* "re-identification." The Commission should take these technologies and their effectiveness into account before dramatically – and prematurely – expanding the scope of recommended privacy procedures and restrictions to non-PII disclosures.

Finally, there is a bedrock principle that appears to be missing from the Commission's otherwise comprehensive and commendable Staff Report – the principle of competitive neutrality. In the evolving Internet marketplace, competition extends across the multiplicity of categories of service providers. Cable operators compete, of course, with other broadband Internet Service Providers ("ISPs"), including telephone companies and, increasingly, wireless service providers. But ISPs also compete with other Internet entities – including entities with access to consumer information – in the highly competitive Internet advertising marketplace.

It is crucially important to a fair, efficient and well-functioning marketplace, as well as to the protection of consumers' privacy interests, that any privacy policies apply uniformly to particular *conduct* or types of data collection that affects the privacy interests of consumers and do not single out particular categories of service *providers* for special treatment. In particular, imposing unique or "heightened" restrictions on conduct simply because it is engaged in by

[3] Staff Report at 43.

broadband ISPs would be especially perverse. As discussed above, ISPs have unique incentives, because of their ongoing relationship with consumers and because of the high cost of losing a broadband customer to a competitor, to be *especially* vigilant in protecting their privacy.

I. A PRIVACY POLICY FRAMEWORK FOR THE INTERNET IS BEST IMPLEMENTED BY INDUSTRY SELF-REGULATION.

The technology of the Internet makes possible the collection, availability and commercial use of information in myriad ways that can affect individual privacy. Different entities in the Internet ecosphere make different uses of consumer information, some of which have a much greater impact on privacy interests than others, and some of which provide greater countervailing benefits to consumers than others. Moreover, these privacy issues are arising in the context of a an Internet marketplace that has, since its inception, continued to offer consumers more and more valuable and exciting new services, content and applications that were unimaginable until they appeared. The economics and the technology of this marketplace are constantly evolving and in flux, and while these may be the best circumstances for innovation and consumer satisfaction, they are the *worst* circumstances for regulatory intervention.

The procedures for adopting and modifying agency rules and regulations – much less the process for enacting and amending legislation – are lengthy and cumbersome, and are hardly suitable for anticipating and addressing issues and problems in as rapidly changing a marketplace as this one. Moreover, the risks of imposing government regulations that miss the mark by failing to anticipate developments in the Internet marketplace are great. The continuing growth of Internet services depends not only on technological advances but also on the underlying economics, which are necessarily evolving along with the technology. To the extent that the economic underpinnings of some Internet services are dependent on arrangements that may, to varying degrees, implicate consumer privacy interests, regulations that unduly and unexpectedly

affect those underpinnings – *i.e.*, rules that have unintended consequences – can have cascading effects on the availability, shape, and value of Internet services.

For example, in recent years, so-called "targeted advertising" has begun to play an increasingly large role in supporting the provision (often without a fee) of valuable web content and services, fostering innovation on the Internet, and promoting growth and employment in the online services sector.[4] The Staff Report acknowledges that "online advertising helps to support much of the content available to consumers online and allows *personalized* advertising that many consumers value."[5] As Chairman Leibowitz has pointed out, advertising targeted at individual households based on information that advertisers may have obtained about such households are "usually good for consumers, who don't have to waste their time slogging through pitches for products they would never buy; good for advertisers, who efficiently reach their customers; and good for the Internet, where online advertising helps support the free content everyone enjoys and expects."[6]

Even though the use of online behavioral advertising is relatively new, it is a particularly important tool for the web, where audiences are scattered across countless sites and transactions

---

[4] *See e.g., "Do-Not-Track" Legislation: Is Now The Right Time?: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. on Commerce, Trade, & Consumer Protection* (statement of Joan Gillman, Executive Vice President and President, Media Sales, Time Warner Cable at 2) (Dec. 2, 2010) ("Gillman Testimony").

[5] Staff Report at 33-34 (emphasis added).

[6] John Eggerton, *Leibowitz: FTC Not Interested in Regulating Behavioral Ads*, Multichannel News, May 12, 2010, *available at* http://www.multichannel.com/article/452585-Leibowitz_FTC_Not_Interested_In_Regulating_Behavioral_Ads.php; *see also In re Information Privacy and Innovation in the Internet Economy*, NTIA Docket No. 100402174-0175-01, NCTA Comments at 2 (June 14, 2010) ("NCTA 2010 NTIA Privacy Comments"). As NCTA explained,

> Targeted advertising, in particular, has many advantages for consumers. Advertising that is more relevant for the consumer is likely to be of more practical value to the consumer. Instead of receiving irrelevant ads, consumers receive information about products and services tailored to their specific interests based on prior purchases, and increasingly through self-managed preference profiles. Customized advertising enables them to make more accurate purchasing decisions in the marketplace, and more businesses, in turn, are empowered to compete by fostering their ability to reach receptive and intended audiences.

Id.

are occurring rapidly. It has become increasingly important to segment audiences on the Internet in order to direct the most relevant ads. Accordingly, online behavioral advertising has become a highly popular method for advertising because of its effectiveness,[7] and its popularity is growing.[8]

But targeted advertising could implicate privacy concerns to the extent that it relies on the identification of types of Internet users that are likely to purchase certain products, and the overlay of those criteria onto groups of actual potential customers – whose identities may or may not be known to advertisers or web publishers. The magnitude of such privacy concerns may vary depending upon the specificity and scope of the personal information, if any, that is collected and used. And the magnitude is important because any such concerns must be balanced against the benefits of such advertising in determining, as a policy matter, whether and to what extent it should be restricted.

Similar balancing of privacy concerns and consumer benefits should also apply to other conduct involving the use of consumer information on the Internet – some of which may implicate privacy interests to a much greater extent than the use of aggregated or anonymous

---

[7] Howard Beales, *The Value of Behavioral Targeting*, at 3, filed by the Network Advertising Initiative, Comment Project No. P095416, at 21 (Apr. 8, 2010) ("Beales Study") ("Behavioral targeting has become an attractive model for advertisers because of its effectiveness. In 2008, Collective Media reported that in a survey of 500 advertisers and agencies, nearly 69 percent used some form of [behavioral targeting].").

[8] Beales Study at 21 ("Industry research service E-marketer reports that spending on behaviorally targeted online advertising reached $775 million in 2008. E-Marketer also projects that by 2012, spending on behavioral advertising in the U.S. will approach $ 4.4 billion, or nearly 9 percent of total ad spending (up from 2 percent in 2006)."); *see also* comScore, *Americans Received 1 Trillion Display Ads in Q1 2010 as Online Advertising Market Rebounds from 2009 Recession*, Press Release (May 13, 2010) ("U.S. Internet users received a record 1.1 trillion display ads during the first quarter, marking a 15-percent increase versus year ago."); *at* http://www.comscore.com/Press_Events/Press_Releases/2010/5/Americans_Received_1_Trillion_Display_Ads_in_Q1_2010_as_Online_Advertising_Market_Rebounds_from_2009_Recession; *2010 Advertising Outlook Improving for All Media Categories* (Apr. 16, 2010) (reporting on a study which found that "[o]nline paid search advertising is expected to increase 16.8 percent" and also noting that an industry group found that "a record $6.3 billion was spent on online advertising in the last quarter of 2009") *at* http://news.suite101.com/article.cfm/2010-advertising-outlook-improving-for-all-media-categories-a226580.

information for targeted advertising. Statutes, rules and regulatory proceedings are altogether too cumbersome, constraining and inappropriate tools for applying such balancing on an ongoing basis to evolving services, technologies and business models. A self-regulatory approach is far better suited to this task.

To be clear, by "self-regulatory," we do not mean "trust us all and leave us alone." There is an active role for policymakers to play – a role that the Commission is playing in this proceeding – in establishing, along with industry stakeholders and interested parties, a policy framework to guide the online gathering and use of consumer information. And industry stakeholders have an active role to play in establishing standards and best practices for applying the principles of that framework to evolving privacy issues.

Indeed, cable ISPs, program networks, and online advertisers have made significant strides in creating robust self-regulatory initiatives that protect consumer privacy while allowing consumers to benefit from innovative advertising. In response to encouragement from the Commission and other agencies, entities interested in online advertising have advanced a number of proposals that address privacy issues in an effective and evolving manner.

In particular, there has been a concerted effort to increase consumer awareness of online advertising methods and create consumer-friendly notice policies. For example, the "online advertising" industry has developed an enhanced notice model, which provides consumers specific information on what company provided the ad, where to find advertising policies, and how to opt-out of targeted advertising in the future.[9] In addition, companies facilitating online

[9] Staff Report at 64 ("An industry group comprised of media and marketing associations has developed self-regulatory guidelines and an opt-out mechanism for behavioral advertising. This group has formed a coalition to develop an icon to display in or near targeted advertisements that links to more information and choices. The coalition has stated that providing consumers with choices about online advertising is essential to building the trust necessary for the marketplace to grow and has pledged to implement this effort industry-wide. In addition, each of the major browser vendors offers a mechanism to limit online tracking, with varying scope and ease of use. These browser vendors recognize the importance of offering consumers choices in this area."; *Id*. at 68

advertising also have developed the ability for users to create anonymous viewing modes for making individual decisions without creating an advertising profile; Mozilla's Firefox browser offers plug-ins for opt-out,[10] and almost all browsers offer an anonymous browsing mode that may be turned on and off. Google and Microsoft also recently announced browser tools that will allow users to opt-out of tracking technologies.[11]

The full range of industry stakeholders should continue to work together to establish best practices and self-regulatory principles, which will likely give consumers the certainty and predictability that they need without the counterproductive and unintended effects of rigid statutes and regulations. Achieving these benefits through a federal self-regulatory policy framework, would, however, be hampered by the concurrent applicability of state privacy laws and the enforcement of privacy policies through a private rights of action. The creation of a patchwork of enforceable state regulations would be unworkable and inconsistent with the push towards a federal baseline privacy framework. And it would be utterly inconsistent with the tailored and restrained self-regulatory approach which, as discussed above, best protects and promotes consumers' interests. Indeed, due to the national, and often international, nature of the businesses and equipment markets, federal law frequently preempts state and local laws in this

---

("For example, at the roundtables, one company described how it shows consumers the categories of advertising associated with them, and allows them to de-select those categories and select additional ones. The panelist noted that, when given this option, rather than opting out of advertising entirely, consumers tend to choose to receive some types of advertising.").

[10] *See* Hayley Tsukayama, *The Circuit: Firefox and Chrome Include Do-Not-Track*, Wash. Post, Jan. 24, 2011 ("Mozilla announced it will put a do-not-track feature in its Firefox browser to allow users to opt-out of online behavioral advertising"), *available at* http://voices.washingtonpost.com/posttech/2011/01/the_circuit_firefox_and_chrome.html.

[11] *See* Byron Acohido, *Google Chrome Will Join Other Browsers With Privacy Tools*, USA Today, Jan. 25, 2011 (reporting that Google's "new tool, Keep My Opt-Outs, strengthens a system set up by the Network Advertising Initiative [and allows] consumers . . . to opt out of being tracked by NAI members" and that Microsoft's new "Tracking Protection feature works much the same as Google's new tool, except that instead of conveying opt-out requests only to NAI members, IE9 will be on the alert for click-stream tracking and targeted ads coming from a list of ad networks – and will block them. The list will be compiled with help from privacy and advertising groups.").

area, especially in matters of technology design.[12] A web site should not have to appear to viewers in different ways depending on where they live.

Enforcement of privacy policies through private rights of action – particularly for class action lawsuits – would be particularly inconsistent with the spirit of adopting a voluntary, flexible framework that protects consumer privacy while promoting innovation. The Final Report should support explicit preemption of state and local laws aimed at regulating information collection and use practices, as well as of common law claims that serve as a proxy for enforcing requirements related to the collection, use, or disclosure of covered information, and of state laws that give consumers or others the right to sue based on purported violations of federal rules.

Indeed, the prospect that class action lawyers will treat privacy notices as contracts and seek to exploit any possible ambiguity as the basis for a lawsuit is a significant contributing factor to the evolution of some privacy notices into lengthy and often legalistic documents. If the Task Force wants to encourage companies to communicate privacy disclosures in more understandable terms, then it must provide protection for good faith efforts to inform consumers, even if such efforts do not exhaust every possible issue. Allowing the fear of class action suits to loom over companies creates a recipe for more legalistic responses, not for the kind of creative efforts that educate and produce informed consent.

NCTA believes that to continue to foster innovation in the online behavioral advertising marketplace, as well as to promote competitive entry for ISPs and others, the Commission should

[12] The federal government recognized early in the life of cable technology that preemptive federal standards were essential both for the nationwide deployment of new networks with rapidly changing technology, and to assure "the ability of the industry to respond to technological changes." *City of New York v. FCC*, 486 U.S. 57, 58 (1988). Congress reaffirmed that approach in the 1990's to assure the continued development of cable technology because "[t]he patchwork of regulations that would result from a locality-by-locality approach is particularly inappropriate in today's intensely dynamic technological environment." H.R. Rep. No. 204, 104th Cong., 1st Sess. Pt. 1, at 110 (1995).

endorse the creation of a competitively neutral "safe harbor" status for all companies adhering to self-regulatory principles developed under whatever policy framework is adopted. Such an approach will help encourage national consistency and promote innovation in products and services and in the protection of personal privacy, as well as support the creation of jobs in this important area of our economy.

II. THE PROPOSED PRIVACY FRAMEWORK IS A STEP IN THE RIGHT DIRECTION BUT SHOULD BE MODIFIED IN SEVERAL KEY RESPECTS TO PROTECT CONSUMERS' PRIVACY INTERESTS AND PROMOTE INNOVATION.

As a framework to guide the development of privacy policy and self-regulatory standards and practices, the staff's three-pronged approach of "privacy by design", "simplified choice", and "greater transparency" is a useful and significant step in the right direction. The staff's abandonment of the long-established distinction between personally identifiable and non-personally identifiable information is, at this point, unwarranted. There is still a significant difference in the risks posed by the gathering and disclosure of PII and non-PII, which should be taken into account in any policy framework. And the staff is perhaps too quick to endorse the implementation of a "Do Not Track" mechanism – a concept that requires further study. But, as a general overview of a reasonable policy approach, the staff's proposal is commendable.

A. The Scope Should Continue To Reflect the Distinction Between PII And Non-PII And Should Be Tailored To Reflect a Continuum of Risks

The staff's proposed privacy framework encompasses a broad scope: it applies "to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device."[13] This approach is based in large part on the perception

[13] Staff Report at 41 ("framework would apply broadly to online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device").

that the distinction between the two categories of data, PII – *e.g*. name, address, Social Security Number – and non-PII – *e.g*. anonymous or de-identified information, has eroded and that information practices and restrictions that rely on this distinction are losing their significance. The staff asserts that the diminishing relevance of PII and non-PII is "due to changes in technology and the ability to re-identify consumers from supposedly anonymous data."[14]

Collapsing the long-held distinction between PII and non-PII data should not be done lightly. The evidence simply does not support dismissal of the efficacy of data anonymization and de-identification techniques to protect consumer privacy or justify a finding at this stage that the scope of privacy protections and disclosures should be expanded to non-PII data.

While some fear that the anonymization of data, even aggregated data, can be readily and easily reverse-engineered, these concerns are based on a few anomalous incidents in which anonymization techniques were poorly executed or data was released indiscriminately. Those few examples, however, do not mean that overall technology does not work. To the contrary, in the vast majority of cases, anonymized data cannot be reverse-engineered and protects the identities of specific users.

There are a wide range of techniques to anonymize and protect information and to minimize the risk that aggregated or anonymized data could be reverse engineered so as to identify an individual. For example, data can be encrypted and hashed, access controls can secure the data, data can be grouped into ranges (such as age ranges rather than birthdays), individual records can be aggregated into groups, contractual limits can restrict the handling, use, and merger of de-identified data. Other federal agencies are increasingly recognizing such

[14] *Id.* at 43.

techniques as effective in protecting personalized data.[15] The National Institute of Standards and Technology ("NIST"), for example, is examining the capabilities of encryption technologies as a means of safeguarding personal information. The FTC's new chief technologist will provide valuable input to the Commission's privacy recommendations, presumably including his assessment of the effectiveness of various privacy-enhancing technologies.[16] Only through a full examination of the types of information collection and usage practices that most concern consumers, the risks associated with those practices, and existing means of minimizing those risks, can information policies be properly targeted towards the practices that create the greatest risk of concrete harm to consumers. Consistent with the staff's desire to support the use of privacy-enhancing technologies,[17] the Final Report should ensure that its policy recommendations do not have the perverse effect of inadvertently *discouraging* privacy-enhancing techniques that would benefit consumers.

Furthermore, the Commission should recognize that the melding of PII and non-PII data for privacy purposes has practical implications in that the distinction between PII and non-PII is critical to how the Internet functions today. Indeed, to put information associated with a particular device or computer on par with information associated with a specific person raises a

---

[15] *See, e.g.*, Erika McCallister *et al.*, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft) – Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-122 (Draft) (Jan. 2009), *available at* http://csrc.nist.gov/publications/ nistpubs/800-122/sp800-122.pdf (noting that the precise techniques and level of protection varies according to the sensitivity of the data being protected and its intended use); Federal Committee on Statistical Methodology, *Statistical Policy Working Paper 22: Report on Statistical Disclosure Limitation Methodology* (Revised 2005), http://www.fcsm.gov/working-papers/spwp22.html (discussing anonymization techniques). The DATA Act, passed by the House last year and introduced in the Senate by Senator Pryor, also recognized the protection afforded by encryption, exempting entities from having to notify affected individuals of data breaches if the data involved was encrypted in accordance with recognized industry standards or best practices. H.R. 2221, 111th Cong. § 3(f)(2)(A) (2009); S. 3742, 111th Cong. § 3(f)(2)(A) (2010).

[16] *See* News Release, FTC, *FTC Names Edward W. Felten as Agency's Chief Technologist* (Nov. 4, 2010).

[17] Staff Report at 52 (discussing staff support for the use of privacy-enhancing technologies, including identity management, data tagging tools, and the use of Transport Layer Security/secure sockets Layer ("TLS/SSL") or other encryption technologies. And noting the use of such technologies should be proportionate to the size of the business and sensitivity of the data at issue.).

number of practical challenges. For example, key identifiers, such as IP addresses, are used to render web pages on an ongoing and persistent basis. Web sites also routinely collect data in order to assess the popularity or desirability of particular features, functions, and offerings. Creating a regime where routine activities such as opening a web page or clicking on a link could result in a barrage of notices will unnecessarily frustrate customers' online experiences and dilute the efficacy of notices.

In any event, NCTA believes that the Commission should focus on tailoring a privacy framework that distinguishes between the risks posed by collection and use of anonymized and aggregated data on the one hand, and PII, on the other, and acknowledge that different types of information collection and usage practices create different risks of harm.

In particular, the Final Report should explicitly acknowledge that the risks presented by the collection and storage of data that does not contain PII are not the same as those associated with personal data that identifies a user and that, in fact, restrictions are unwarranted if data is aggregated, encrypted, or otherwise rendered unidentifiable as to a specific individual. Suggestions that a privacy framework accord the same level of privacy protection to the collection or use of such data as they would to information that is specifically associated with an identifiable user are unsupported by any empirical evidence that they present the same risks. Nor has it been shown that consumers accord the same level of concern over the privacy of information that *cannot* be identified with them, as they do toward information that *can* be identified with them.

Therefore, we urge the Commission to adopt a policy approach that continues to recognize the differences between PII and non-PII, and preserves incentives to anonymize or de-identify data to protect consumers. Such an approach will encourage the development and use of

safe harbors as an alternative to more restrictive privacy requirements.

B. The Cable Industry Employs Privacy By Design

The Staff Report recommends the principle of "privacy by design," namely, that companies "should incorporate substantive privacy and security protections into their everyday business practices and consider privacy issues systemically, at all stages of the design and development of their products and services."[18] This is a principle that NCTA readily endorses – because the cable industry has already embraced it since protection of our customers' privacy is integral to our companies' relationship with their subscribers.[19]

From the cable industry's perspective, consumer choice and control over private data, providing clear notice and transparency of data practices, and protecting sensitive data are paramount to our companies' efforts to protect their customers' privacy.[20] This is not surprising. As explained by Kyle McSlarrow, President & CEO of NCTA, the cable industry "views the protection of our customers' privacy as a fundamental part of our relationship with our customers and central to the success of our businesses."[21] Moreover, cable systems operate in a highly

---

[18] *Id.* at 44.

[19] *See, e.g.*, Gillman Testimony at 1-2 ("The bedrock foundation of our business is our relationship with our subscribers. We operate in a highly competitive marketplace, and our ability to succeed depends upon winning and retaining the trust of our customers. Our customers rely upon us to serve as a trusted medium for accessing and delivering content and services that reflect consumer tastes and preferences. It is our job to preserve and strengthen that trust, while continuing to innovate and introduce the benefits of new network technologies and capabilities.").

[20] *See* Testimony of Kyle McSlarrow, President and CEO, NCTA, on Communications Networks and Consumer Privacy: Recent Developments, H. Energy and Commerce Subcomm. on Communications, Technology & the Internet, Apr. 23, 2009 at 3 (discussing that achieving and sustaining subscribers' trust requires adherence to a privacy framework addressing four main principles: 1) giving customers control; 2) providing transparency and notice; 3) safeguarding personal information and 4) providing customers with value; also noting that special care should be given to sensitive data, such as health or financial information, as well as protecting children online); see also Federal Communications Commission Public Notice, *In re A National Broadband Plan for Our Future, GN Docket No. 09-51, Comments Sought on Privacy Issues Raised by the Center for Democracy & Technology*, NBP Notice # 29, DA 10-62, NCTA Comments, Jan. 22, 2010.

[21] Letter from Kyle McSlarrow, President & CEO, NCTA, to Chairman Boucher and Ranking Member Stearns, H. Comm. on Energy and Commerce, Subcomm. on Communications, Technology & the Internet at 8 (June 4, 2010).

competitive marketplace, and their ability to succeed depends on winning and retaining the trust of their subscribers.[22]

Cable system operators providing video services have long operated under a comprehensive framework of protecting their customers' privacy pursuant to Section 631 of the Communications Act.[23] Enacted in 1984, this provision:

- requires cable operators to provide annual written notice to consumers of the nature of personally identifiable information ("PII") collected, including clearly and conspicuously describing how it is used, disclosed to others, and maintained;
- prohibits cable operators from collecting PII over the cable system without prior customer consent, except as necessary to render service and detect service theft, and from disclosing PII without prior customer consent, except as necessary to render services or conduct other legitimate business activities related to rendering service;
- provides detailed requirements governing how subscriber records may be disclosed pursuant to court order;
- requires that subscribers be given access, at reasonable times and convenient locations, to all PII that is collected and maintained, and a reasonable opportunity to correct any errors in PII; and
- requires cable operators to take "such actions as are necessary" to prevent unauthorized access to PII, including destroying it if it is no longer necessary for the purposes for which it was collected and there are no pending court orders or requests for access to such information.

In providing digital voice service, cable providers comply with the privacy protections of Section 222 of the Communications Act regarding customer proprietary network information ("CPNI").[24] Between Section 631 and Section 222, the cable industry already operates in an enforceable privacy framework that substantively embodies well-recognized fair information principles.[25]

---

[22] *See id.*

[23] 47 U.S.C. § 551.

[24] 47 U.S.C. § 222; 47 C.F.R. Part 64, Subpart U.

[25] *See, e.g.*, Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

Cable companies are exploring new broadband business models and network technologies with the full appreciation that new services must be deployed consistent with our long-standing commitment to protect customers' personal information and facilitate well-informed privacy decisions.[26] No business which seeks to preserve and maintain a long term customer relationship benefits from disregarding customer privacy concerns and discarding their trust and confidence.[27]

As the Staff Report recommends, "[c]ompanies that maintain information about consumers should employ reasonable safeguards- including physical, technical, and administrative safeguards – to protect that information."[28] Cable operators already employ many such measures, including designating chief privacy officers and other individuals responsible for privacy concerns; performing background checks of employees; requiring ongoing training for employees that handle sensitive data; anonymizing customer data; and implementing data retention and deletion policies.[29] Cable operators also work to ensure that all equipment, including computers, servers, and any other assets used to collect, store, or process data is

---

[26] *See, e.g.*, Gillman Testimony at 1 ("Presently, Time Warner Cable does not engage in targeted online advertising, as an ISP, based on our subscribers' web surfing activities, or target ads based on our consumers' search queries, web surfing, or related aspects of their usage. As we examine new advertising business models, Time Warner Cable is committed to ensuring the protection of our customers' privacy."); *see also In re Information Privacy and Innovation in the Internet Economy*, NTIA Docket No. 101214614-0614-01, NCTA Comments at 2 (Jan. 28, 2011) ("NCTA 2011 NTIA Privacy Comments"); NCTA 2010 NTIA Privacy Comments at 5.

[27] As Commissioner Kovacic explains, firms have economic incentives to meet consumers' demand for privacy. Staff Report, Kovacic Statement at D-2 ("In its current form, the report understates the economic incentives that firms have today to meet consumers' demand for privacy. For example, large data breaches can have negative financial consequences for firms. The increasingly widespread use of privacy controls such as NoScript and TACO – a development the report cites – might suggest that firms are working to meet consumer demands for privacy.").

[28] Staff Report at 44-45.

[29] *See, e.g.*, Cox, *Annual Notice to Cox Customers, Your Privacy Rights as a Cox Customer and Related Information* ("We keep only the personal information needed to serve you, treat it as private, use it only for what we offer you, do not sell it to others, work to keep it secure and destroy it when no longer needed. We will give you clear, prior notice and the right to choose, if a service requires an exception to this promise."), *available at* http://ww2.cox.com/aboutus/policies/annual-privacy-notice.cox.

secured against unauthorized physical access. Employees are granted access to sensitive customer data only on a need-to-access basis. Cable operators also take steps to ensure network security, including requiring authentication for access to data; controlling access to data by using tools such as systems that automatically log attempts to access data; implementing workstation and perimeter security controls; and periodically assessing security systems. Finally, cable operators implement precautions for data transmission security by employing industry-standard encryption measures.

Privacy and security controls related to cable broadband access have become standard practice in protecting consumers from malware, spyware, viruses, and other privacy invasions.[30] For example, many cable operators offer security software for free, or at a low additional cost to broadband subscribers.[31] Norton Security Suite, offered by Comcast to its broadband subscribers, provides features including: (1) firewall protection; (2) anti-virus protection; (3) identity security; and (4) parental controls.[32] Similarly, the McAfee Security Suite, offered by cable operators such as Cox and Suddenlink to broadband subscribers, provides many features including anti-virus scanning; anti-spyware, anti-phishing, and anti-spam software; firewall protection, parental controls; and identity protection that requires confirmation before personal

---

[30] *See, e.g.*, Federal Communications Commission proceeding, *In re A National Broadband Plan For Our Future ("NBP")*, GN Docket No. 09-51, Time Warner Cable Comments at 13 (June 8, 2009), citing a variety of privacy tools; Comcast Comments at 25 (June 8, 2009); NCTA Comments on NBP Notice #29, January 13, 2010.

[31] *See, e.g.*, Comcast, *Comcast.net Security*, *at* http://security.comcast.net/get-protected/index.aspx, (last visited Feb. 3, 2011); *Cox, Overview: Cox Security Suite, at* http://ww2.cox.com/residential/hamptonroads/internet/cox-security-suite.cox?campcode=xl_internet_3_security-suite_1001 (last visited Feb. 3, 2011); Time Warner Cable, *High-Speed Online*, *at* http://www.timewarnercable.com/Northwest/learn/hso/ (last visited Feb. 3, 2011); Cablevision, *Optimum Online*, *at* http://www.optimum.com/online/features/index.jsp (last visited Feb. 3, 2011); BendBroadband, *Protect Your Precious Data, at* http://mybendbroadband.com/provisioning/security/index.php?sc_cid=dir_security_holidaycall (last visited Feb. 3, 2011); Suddenlink, *Suddenlink Security Suite, at* http://www.suddenlink.com/internet/security.php (last visited Feb. 3, 2011).

[32] *See* Comcast, *Norton Security*, *at* http://security.comcast.net/get-protected/index.aspx (last visited Feb. 11, 2011).

information is sent from a subscriber's computer.[33]

Some cable operators also offer online resources to provide information to subscribers about additional steps they can take to protect their privacy online. For example, Comcast provides an entire website devoted to privacy concerns.[34] On this site, subscribers can learn about ways to protect themselves online through FAQs, up-to-date security alerts, and information about their free anti-virus packages. Cox offers a variety of educational tools concerning online security, including its "Take Charge" program that is dedicated to parental education.[35] Cable companies have also taken steps to promote online privacy in other ways. For example, Time Warner Cable is supporting academic research in the area of privacy issues related to online advertising.[36] At the same time, Cox has focused on security issues for adolescents by hosting annual summits on Internet safety in conjunction with the National Center for Missing and Exploited Children.[37] This sort of "privacy by design" by cable operators will surely continue, informed by evolving concepts, whether or not it is part of a broader government-endorsed policy framework.

C. Simplified Choice Should Focus on Uses Where Consent is Not Needed Rather than Freezing Certain Approved Practices

The second element of the proposed framework, simplified choice, is a further step in the

---

[33] *See* Cox, *Overview: Cox Security Suite*, *at* http://ww2.cox.com/residential/hamptonroads/internet/cox-security-suite.cox?campcode=xl_internet_3_security-suite_1001 (last visited Feb. 3, 2011).

[34] Comcast, *Comcast Security*, *at* http://security.comcast.net/get-smart/security-trends/news-and-alerts.aspx (last visited Feb. 3, 2011).

[35] *See* Cox Communications, *Take Charge! Tips and Tools*, *available at* http://www.cox.com/takecharge/tips_tools.asp.

[36] *See* Press Release, Time Warner Cable, *Time Warner Cable Presents New Research Program Awards* (Dec. 15, 2010), *available at* http://ir.timewarnercable.com/phoenix.zhtml?c=207717&p=irol-newsArticle&ID=1508036&highlight=privacy.

[37] *See* Press Release, *Cox Communications, Cox Survey Shows 46 Percent of Teens Allow Unrestricted Access to Their Online Profiles and 62 Percent Don't Check with Parents Before Posting Photos* (June 15, 2010), *available at* http://cox.mediaroom.com/index.php?s=43&item=489.

right direction. Finding that "consumers face considerable burdens in understanding lengthy privacy policies and effectively exercising any available choices based on those policies,"[38] the staff calls on companies to provide consumers with simplified, meaningful choice, but allows for a limited set of data practices for which choice is not necessary. In proposing "a streamlined choice model," the staff's goal is to "foster clearer expectations for consumers and businesses regarding the types of practices for which choice should be provided."[39]

The emphasis on simplifying choice stems from the Commission's finding that the existing notice-and-choice model – in which businesses provide notice of what information they collect from consumers and how they use it and give consumers choice about how information collected from them may be used – is not working. The Staff Report finds privacy policies "have become longer, more complex, and in, too many instances incomprehensible to consumers."[40] Although the Staff Report minimizes the role that notice and choice and harm-based models continue to play in a privacy regime, it is not clear that consumers fail to understand the choices presented to them in privacy notices, or that they are otherwise unaware of the trade-offs associated with sharing information, when the notice given is properly and appropriately clear and understandable. Consumers frequently become more comfortable with the use of personal information as they gain experience with it and enjoy the benefits associated with it. Frequent shopper and other "affinity" cards, bar codes, and online purchases, for example, once raised substantial concerns but are now regarded as commonplace. Privacy policy will benefit from a better understanding among all stakeholders of changing consumer expectations and risk tolerance in the context of innovative new uses of personal information.

---

[38] Staff Report at 52.

[39] *Id.* at 53.

[40] *Id.*at 19.

Nevertheless, the cable industry is constantly working to provide simple and easily understandable privacy policies for its customers.[41] Operators frequently review and revise their privacy policies consistent with their annual obligation to notify customers of privacy protections. However, we recognize the desire to improve privacy notices and disclosures across the array of services and entities engaging consumers on the Internet.

1. "Commonly Accepted Practices"

The staff proposes to simplify consumer choice by focusing consumers' attention and choices only on disclosures of information that should matter to them. Specifically, it proposes to exempt from its simplified choice requirements any "commonly accepted practices." This is a constructive idea – provided that "commonly accepted practices" are identified in a competitively neutral and ongoing manner based on evolving consumer expectations of what is a common practice.[42]

Attempting instead to identify in advance a static list of such practices poses the risk of freezing pre-approved "accepted" practices in place, potentially stifling the evolution of more effective or efficient practices or technologies. It also suggests that any practice that is not identified on the list is presumptively unacceptable for consumers. While there are benefits to

---

[41] As explained by Gerard Lewis, Vice President, Deputy General Counsel & Chief Privacy Officer, Comcast Cable Communications:

> In the rapidly changing online environment, we want consumers to have consistent, clear notice about our website privacy practices and the ads they see. That's what this pilot program with TRUSTe is intended to do. We're pleased to continue our longstanding relationship with TRUSTe to help give our customers that confidence when they visit and use our websites.

Press Release, TRUSTe, *TRUSTe Launches Pilot of Behavioral Advertising Notice and Choice Program* (Jan. 26, 2010) (discussing TRUSTe's pilot program offering website publishers a "plug and play" widget that provides consumers with an easily accessible and transparent notice of advertising practices and the ability to exercise opt-out choices for the ad networks and other third parties that deliver ads on those sites), *available at* http://www.truste.com/about_TRUSTe/press-room/news_truste_oba_pilot_announcement.html. This program is a model for the kinds of self-regulatory programs now being implemented by the Internet advertising industry.

[42] As discussed below, the competitive neutrality issue arises when a certain way of collecting identical information is treated differently in terms of "commonly accepted practices" based on differences among industries (*i.e.,* collection of information on a first-party basis is treated differently based on technology employed rather than based on the uses of the information being collected).

identifying at the outset certain practices that are already clearly within the ambit of what consumers would reasonably expect, it should expressly be stated that the array of such practices will evolve over time as customer familiarity and exposure evolves, without the need to amend a static list. Consumers could be educated about the *kinds* of uses to which their data may be subject, rather than every possible such use.[43] Calling such practices "legitimate business practices" may more accurately convey this goal.[44]

A general example of practices that can be identified at the outset as outside the scope of choice requirements would be the collection of information that is not subsequently disclosed to third parties. It would unnecessarily impede the provision of basic Internet-based services and features to require entities to obtain consent in circumstances where they are only collecting, but not disclosing to any third parties, information. An entity should only be required to provide notice to consumers if it is disclosing information to unaffiliated third parties, regardless of technology used or nature of the entity directly collecting that information from the end user.

The staff also asks how the proposed framework should handle the practice of "data enhancement," whereby a company obtains data about its own customers from other sources, both online and offline, to enrich its databases.[45] The cable industry believes that such practices should not trigger the need to provide consumer notice. If notice and choice is to be offered at all, in this chain of relationships, it should be offered by those who initially collect this data from consumers and share it with database companies that make it available for marketing purposes –

---

[43] For example, the Cable Act requires cable operators to provide customers notice at the beginning of a service arrangement and annually thereafter about the "nature of the use" of personally identifiable information. 47 U.S.C. § 551(a)(1)(A).

[44] An example of such a "legitimate business practice" would be when a company retains information provided by a customer and uses that information to market new services of interest to that customer, without sharing that information with any third parties.

[45] Staff Report at 57.

often to direct mail marketers, not just Internet advertising or other companies. Enhancing knowledge of a company's customer base with demographic and other generalized, commonly-available information, both online and offline, is a routine practice for companies to understand and serve their customers.

Where consumers are presented with choice, the Staff Report recommends that companies offer easy-to-use choice mechanisms, and to be most effective, such mechanisms should be provided at a time and in a context in which the consumer is making a decision about his or her data. The staff rightfully recognizes that different mechanisms for obtaining opt-in and opt-out consent can vary in their effectiveness. For example, the staff notes that "a clear, simple and prominent opt-out mechanism may be more privacy protective than a confusing, opaque opt-in" mechanism.[46] The time and effort required for consumers to understand and exercise options is important to achieving informed consent.

Moreover, the goal of "simplified choice" should look to privacy protection tools that an industry already has in place and on the near horizon, that have been designed to address privacy issues in an evolving and effective manner. Many roundtable participants provided information on the various tools currently being offered and in development that will more fully engage consumers in their privacy choices and give them the ability to control their choices.[47] And, as previously noted, the staff is well aware that there are new privacy-enhancing technologies and

---

[46] *Id.* at 61.

[47] *See, e.g.*, Comments filed in response to FTC's Privacy Roundtables, FTC Project No. P095416, Microsoft Comments at 15 (discussing a technical method used by Microsoft called a one-way cryptographic hash which is used to separate search terms from account holder's personal information in a way that prevents them from being easily recombined); EPIC Comments at 5 (calling for the Commission to further explore the use of anonymization techniques that provide for de-identification of data that cannot be combined with other info for re-identification to protect consumers); Lee Tien, Transcript of FTC Second Roundtable on Exploring Privacy, Technology & Policy Panel at 302, 330 (discussing Tor, a privacy-enhancing tool used for anonymous web browsing and another crypto-based system available in the European Union for automatic tolling in transit systems with complete anonymity).

consumer information management tools that seek to make consumers more aware of data collection practices and make it easier for them to set their privacy preferences. These efforts are designed to offer consumers the choice at the time and in a context in which the consumer is making a decision about his or her data (or engaging the company).

In addition, as discussed above, companies facilitating online advertising also have developed the ability for users to create anonymous viewing modes for making individual decisions without creating an advertising profile; and almost all browsers offer anonymous browsing modes and some are offering opt-out mechanisms for control of tracking technologies consistent with customer preferences.[48] And privacy and security controls related to cable broadband access have become standard practice in protecting cable consumers.

These developments and activities have enabled the online advertising industry to offer innovative consumer protection mechanisms to preserve consumer privacy, which in turn has spurred consumer confidence, and permitted online advertising to grow to meet the needs of the greater Internet community.

2. The "Do Not Track" Choice Mechanism

The Staff Report gives special attention to the "Do Not Track" choice mechanism, given its potential to provide a more uniform and comprehensive consumer choice mechanism for online behavioral advertising.[49] Specifically, as described by staff, the mechanism would enable a consumer to place a setting similar to a persistent cookie on his or her browser and convey that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements.[50] According to the Staff Report, for such a mechanism to be

---

[48] *See supra* at 11.

[49] Staff Report at 66.

[50] *Id.*

effective, there must be an enforceable requirement that sites honor those choices. It suggests that such a mechanism "could be accomplished by legislation or potentially through robust, enforceable self-regulation."[51]

Proposals to implement "Do Not Track" mechanisms raise several important questions that must be fully explored before such mechanisms are imposed by law or regulation. These questions include the limited effectiveness of these mechanisms; the potential unintended consequences of Do Not Track on consumers;[52] and the impact of Do Not Track on the advertising that funds free Internet content, Internet commerce, and jobs.[53] Indeed, the Staff Report recognizes that there are several important issues with respect to such a mechanism.[54] The Commission should obtain a deeper understanding of the impact of Do Not Track on

---

[51] *Id.*

[52] For example, there is a fundamental question as to how a "Do Not Track" mechanism would distinguish beneficial tracking used to optimize websites or police against malicious and fraudulent activity from other types of tracking? Depending on how many people use a particular mechanism to comprehensively opt out of targeted advertising, could such activity result in multiple log-ins, "pay walls," or additional pop-up and overlay advertising?

[53] Many of the assumptions underlying the Staff Report's "Do Not Track" recommendation beg further evaluation. For example, as Daniel D. Castro of the Information Technology and Innovation Foundation recently explained in Hill testimony,

> One problem with the term "tracking" is that it is an overly-broad term that does not correlate to a specific technical activity. Many activities could be considered tracking: setting unique identifiers for users in their web browser cookies, logging IP addresses on a server, monitoring IP packets over a network, and building unique profiles for users on a website. Policymakers should remember that companies collect data for many purposes besides providing targeted advertising. Google, for example, uses data provided by consumers for everything from tweaking its search results to developing its free email service to improving its speech-to-text engine that is now used on mobile phones. Many websites use consumer data to deliver personalized services to deliver content to users based on information they, or a third party, know about the user. . . . Even when used for online advertising, companies do not just collect data to deliver customized user ads. Online advertisers use logs, for example, to create an audit trail so that they can prove to their customers that they have delivered the number of ads that they have sold and prevent criminal activity, including click fraud.

"Do-Not-Track" Legislation: Is Now The Right Time?: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. on Commerce, Trade, & Consumer Protection (statement of Daniel D. Castro. Senior Analyst, Information Tech. & Innovation Found. at 5) (Dec. 2, 2010).

[54] In particular, the Staff Report explains that any consumer choice mechanism for online behavioral advertising "should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value." Staff Report at 67.

growth, revenue, and employment in the online services sector – as well as its impact on the continued availability of content on the Web – before endorsing such an approach. Furthermore, the Commission must consider carefully the market implications of endorsing browser companies or any other stakeholders as gatekeepers of consumer choice in this regard.

As the Staff Report acknowledges, consumers are already being provided more and more refined tools – web icons, easy opt-out, browser plug-ins, and anonymous viewing modes – for making individual decisions about which sites may and may not collect information, and when.[55] Such market-based approaches, paired with other self-regulatory means, should be allowed to further develop as the Commission studies the implications of a Do Not Track mechanism. Such an approach is critical, because the stakes are high:

> Depending on how do-not-track is implemented . . . it could be a blunt instrument that upsets consumer expectations and negatively affects advertiser-supported content businesses (such as newspapers, magazines, and video – TV and movies) – even as these industries try to figure out how to create viable online business models. Do-not-track could hinder job creation within the advertising industry and by websites that rely on advertising revenues. It may also deter the provision of free online advertiser-supported content and inhibit innovation and the development of new services.[56]

In sum, the "simplified choice" element of the privacy framework needs to be aimed at ensuring that consumer choice takes into account not only privacy concerns but also the potential reasons for and benefits of disclosure of consumer information. Opt-in, opt-out, and "Do Not Track" concepts all need to be implemented in a way that does not "nudge" consumers toward ignoring legitimate privacy concerns (by making the notice and choice process too cumbersome and confusing so that consumers ignore it) or toward reflexive refusal to allow any disclosures, even if such disclosures are compatible with privacy interests and beneficial to consumers and

---

[55] *Id.* at 63-64.

[56] Gillman Testimony at 4.

the economics of the Internet.

D. Greater Transparency Should Account For Current Industry Practices And Should Be Tailored To Specific Consumer Interactions.

The final element of the proposed framework is greater transparency of companies' data practices. The staff finds that consumers are often unaware of how and for what purposes, companies collect, use and share data about them. The report proposes several measures that companies should take to make their data practices more transparent to consumers, notably providing choice mechanisms in a prominent, relevant and easily accessible place for consumers and adopting shorter clearer and more standardized privacy notices to enable better comprehension and comparison of privacy practices.

As discussed above, while the pursuit of greater clarity and consumer-friendly notice on the collection and use of information is a sensible policy objective, we caution against imposing specific language or disclosure requirements. Internet-related businesses need flexibility to tailor notice content and delivery mechanisms to the particular context of information collection and to the needs of their subscriber base.

Moreover, the scope of the proposed disclosure requirements could negate efforts being made by Internet businesses to simplify privacy notices and choices for consumers. The transparency policy should be appropriately targeted to allow for maximum flexibility and innovation. The cable industry has already embraced privacy by design mechanisms and has dedicated substantial efforts to simplifying notice and choice mechanisms for their subscribers.

Recommendations to enhance consumer-friendly notice can be more readily and effectively implemented in a framework of regulatory restraint that offers flexibility for innovation and experimentation, rather than via "one size fits all" regulatory mandates. This approach would also allow companies to use a variety of creative educational tools to educate the

public, such as online videos, Video-On-Demand training, live Q&A sessions, or other means – rather than being shoehorned into a government-mandated approach that may be outdated as soon as rules are released. For the cable industry, preserving flexibility over standardized disclosures is especially critical since cable operators offer multiple services over the same platform. Standardizing service-specific rules could result in cable operators being subject to multiple, potentially conflicting and duplicative disclosure obligations. This would be unfair to cable operators and highly confusing to their subscribers.

Indeed, any highly specific disclosure requirement poses the risk of causing substantial customer confusion. Most likely, consumers will ignore overly detailed notices undermining the very purpose of the notice.[57] As noted above, a regulatory regime where routine activities such as opening a web page or clicking on a link results in a barrage of notices, for example, will unnecessarily impede customers' online experiences and dilute the efficacy of notices. In contrast, self-regulation and industry best practices allow companies to take into account the time and effort required for consumers to understand and exercise the options important to their informed consent.

The staff also asserts that "transparency and consumer choice are undermined when companies change their policies with respect to their use of previously-collected data."[58] It proposes that companies provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected. Some form of opt-out consent is preferable to an express opt-in consent regime, for

---

[57] The staff has not proposed rigid purpose specification and use limitations in privacy notices. But the staff noted that "the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity." Staff Report at 20. We caution that adding another layer of purpose and use limitations may offer nothing more than information that is already addressed in a clear and transparent notice.

[58] *Id.* at 76.

situations where online entities materially change privacy practices for information collected from the customer under a previous privacy policy or where they want to share it for purposes not previously disclosed (and which a reasonable person would not expect based on prior privacy notice). Requiring narrow purpose specification, however, may mean sending frequent updated notices concerning the use of data, which may only unnecessarily confuse and alarm customers. Stringently prohibiting companies from deviating from initial uses would also hinder the development of innovative technologies. Additionally, if the distinction between PII and non-PII were to be erased, and such notices were to be required for use of anonymous or de-identified data, this would be counterproductive.

The staff should also take into consideration that it is not building on a blank slate here. As previously noted, there are other privacy regimes in place which require detailed notices. Removing fully anonymized or de-identified data from notice and choice would avoid this issue and further increase industry incentives to minimize privacy risks and avoid developing data sets attached to known identities.

Finally, in the interests of achieving greater transparency, the staff calls upon all stakeholders to work to educate consumers about commercial data privacy practices.[59] The cable industry wholeheartedly agrees that raising consumer awareness about data practices, in conjunction with the foregoing privacy protections, is an essential component of the privacy framework. By virtue of cable's direct relationship with customers, our companies are providing tools to educate consumers about privacy and are prepared to work with government agencies and through industry-driven initiatives to enhance consumer education.

[59] *Id.* at 78.

III. COMPETITIVE NEUTRALITY SHOULD BE A BEDROCK PRINCIPLE OF THE GOVERNMENT'S PRIVACY POLICY.

Finally, there is a key principle that is not addressed in the privacy framework: the principle of competitive neutrality. The Commission should make it a high priority to ensure that privacy guidelines do not unwittingly become a means by which some online advertising business models obtain advantages over others. In a nascent and highly dynamic market, any regulation that favors or disfavors one technology or business model over another could seriously thwart innovation and the development of new business models that could benefit consumers, content providers, and advertisers, by prematurely locking market participants into one sanctioned approach. Moreover, limiting online advertising to specified designated permissible techniques would deter new entry, and limit competition.

While the Staff Report lauds the importance of consumer information in today's digital economy and acknowledges that "companies are using this information in innovative ways to provide consumers with new and better products and services,"[60] it proposes to restrict one player in the Internet ecosystem, ISPs, with unique privacy burdens that could impede their ability to fully participate in the digital economy. Ironically, ISPs – entities least involved in online behavioral advertising or the practices that have sparked renewed privacy concerns among policy-makers – are singled out for special treatment when they engage in the collection of data across websites for marketing purposes. Even if such activity is done by a single party and not shared with others, the data practice would generally be taken "out of the category of 'commonly-accepted practices' for which companies do not need to provide choice."[61] The staff cite an ISP's use of so-called "deep packet inspection" ("DPI") as an example where consent

[60] *Id.* at i.

[61] *Id.* at 55.

would be required, noting that it is unlikely consumers would anticipate ISP monitoring of all of the online activity in order to create detailed profiles of them for marketing purposes. The Staff Report further asserts that DPI warrants "enhanced consent" or "heightened restrictions" due, in part, to the alleged lack of competition among residential broadband ISPs.[62]

As an initial matter, there is no factual basis to impose heightened notice and consent requirements on ISPs which have not been extensively involved in online behavioral advertising and therefore are not the cause of whatever practices policy-makers may decide justify regulation.[63]

But even if ISPs were full-fledged players in the targeted online advertising business, as a policy matter, the government should not subject different entities involved in online behavioral advertising to different types of notice, consent or other obligations, depending upon the type of technologies they employ. This is particularly true given the convergence of media; where there is often no longer any meaningful distinction between the services offered via different delivery mechanisms – content can be accessed, for example, over cable television, satellite TV, Internet TV and mobile devices – it does not make sense to establish policies that make such distinctions.

---

[62] Staff maintains that enhanced consent or even more heightened restrictions for DPI are called for "because of the scope of the information collected about consumers and the inability of many consumers to discontinue broadband service." *Id.* at 62. The staff further asserts that DPI warrants special concerns "because of the limited level of competition among residential broadband ISPs." (citing the FCC's finding that approximately 96% of the U.S. population has at most two wireline broadband providers and perceived barriers to switching ISPs, such as cost and inconvenience) *Id*. As discussed, *supra,* cable operators compete with other major service providers at all levels of their video, Internet, and telephone business and consumers have a wide array of choice among providers and exercise those choices everyday by switching providers. To the extent ISPs compete with other dominant platforms and applications, a privacy framework that lacks competitive neutrality could result in situations where others engaged in advertising activities with comparable information may do so without offering consumer choice, while ISPs are subject to a higher standard. Consumers could be left guessing when they are protected and when not, which is not what the Commission's privacy framework is intended to accomplish.

[63] *See, e.g.*, Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, Wall St. J., Oct. 18, 2010, *available at* http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

The FTC should avoid endorsing privacy standards that vary according to an entity's technology or role in the marketplace.

In particular, by imposing more aggressive regulation on technologies used by network providers than on other technologies that comparably affect privacy interests, the government would create competitive disparities and market inefficiencies that limit choice by consumers and advertisers. Such a distortion is wholly unnecessary where, as here, there is no evidentiary basis for such a distinction. There is no evidence that consumers regard certain tracking approaches as more or less problematic or invasive than others, and the staff does not cite any examples of consumer harms stemming from particular tracking practices. Rather than according some online entities artificial business advantages, the framework should provide all entities involved in online advertising the opportunity to use any technology or approach, provided that it offers the necessary security and privacy for consumers. Accordingly, the Commission should focus on the permissible use of data, not which technology is used to collect and store it, and in any policy framework should not – explicitly or implicitly – endorse disparate treatment of different models. More important than *how* PII is collected is whether the entities that collect PII can be held *accountable* for their use of that information.

The cable industry has a long history of accountability for protecting the privacy interests of its customers. As described above, long before the advent of commercial Internet service, cable operators operated within the federal privacy regime and cable companies recognize and value their direct relationships with customers.[64] Contrary to the staff's view, cable systems operate in a highly competitive marketplace in the provision of video, telephone, *and* Internet service, and their ability to succeed depends on winning and retaining the trust of those

[64] 47 U.S.C. § 551 (Cable Act provision mandating the protection of subscriber privacy).

customers. As such, cable companies must take special care with their customers' personally identifiable information to protect those relationships. As new business models and new network technologies have developed, cable operators have ensured that they are deployed in a manner that respects their customers' privacy and they will continue to do so.

In their role as Internet service providers, many cable operators are exploring advanced advertising in developing new and innovative products and services for their customers. Interest-based advertising has many advantages for businesses and consumers. Advanced advertising empowers businesses to compete by fostering their ability to reach receptive and intended audiences. This, in turn, helps preserve and expand the content and services offered over the Internet. Indeed, advertising is the economic engine of the Internet.

As the Commission establishes a privacy framework in an evolving 21st century digital marketplace, it should aim to encourage the panoply of competitive service providers to continue to innovate while protecting consumers' legitimate privacy interests. ISPs have the potential to enhance competition in the online advertising market in many ways, by introducing alternatives to the "cookie-based" business models prevalent today. The privacy framework should provide consistent rules for the same data collection process or function, regardless of the type of company or industry involved. This will give consumers certainty and predictability.

For example, if "first party marketing" does not require consent, it should not matter what type of company is involved or what type of technology is used. Similarly, if companies can gather operational information as a "commonly-accepted practice" that does not require consent, it should not matter what tool is used – there should be a simple uniform approach to those activities. If there is a basis for concern about a particular tool, such as DPI, those concerns should be dealt with separately with specific disclosures or other notice. But parties using

functionally similar practices in the collection, use and disclosure of covered information should be subject to similar privacy requirements forged through an accountable self-regulatory regime.

In the context of ensuring competitive neutrality, the Commission should be mindful of the subset of existing regulatory frameworks that certain businesses in the communications sector operate under today. To the extent policy-makers move to a national privacy framework, they should recognize that different privacy regimes are in place today (*e.g*. cable, telecommunications) and their recommendations should be designed to avoid multiple and unequal sets of privacy obligations. Simply applying a new privacy framework across the board to all entities in the Internet ecosystem would disserve competitive neutrality unless stove-piped rules that apply to competing businesses are replaced with uniform rules. The government reconciling existing obligations under the current regulatory frameworks in the sector will not achieve a competitively neutral outcome.

In sum, disparate privacy standards that vary according to an entity's business model, technology, or status in the marketplace could deter new entry, and thereby stifle innovation and development of new business models that could benefit consumers, content providers, and advertisers. The Commission's emphasis should be on particular activities or practices that require clear and easy-to-use notice and consent, rather than the entity or technology involved (whether DPI, browser-based, or other technique). Adopting different privacy policies based on particular online advertising business models or technologies in the abstract would disserve consumers and undermine competition in the advertising marketplace.

CONCLUSION

A privacy framework for the 21st century should be carefully tailored to balance the privacy interests of consumers with the beneficial uses of consumer information to support the complex Internet ecosystem. To achieve this balance while avoiding the unintended consequences of unduly broad restrictions, any such framework should continue to recognize the differences between PII and non-PII; preserve incentives to anonymize or de-identify data to protect consumers; focus on simplifying consumer choice with clear principles over static practices; and rely on existing and emerging industry self-regulation. And first and foremost the government should adhere to a policy of competitive neutrality in developing a privacy framework for the future.

Respectfully submitted,

Rick Chessen
Michael S. Schooler
Loretta P. Polk
Stephanie L. Podey
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222 -2445

February 18, 2011