U.S. DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Information Privacy and Innovation in the Internet Economy	))	Docket No. 101214614–0614–01

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

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

January 28, 2011

TABLE OF CONTENTS

U.S. DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Information Privacy and Innovation in the Internet Economy	))	Docket No. 101214614–0614–01

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA")[1] hereby submits its comments in response to the questions and comments solicited in the Department of Commerce's Internet Policy Task Force's ("Task Force") Green Paper on online privacy.[2] NCTA supports the Task Force's emphasis on the complex and dynamic digital economy; its recognition that the spectacular growth of digital commerce is the result not only of the innovation of Internet entrepreneurs but also of the wisdom of public policy-makers in avoiding prescriptive rules and relying on industry self-regulation; and its acknowledgement that some uses of consumer information are essential to delivering services and applications over the Internet and that others, such as targeted, interest-based advertising, can be beneficial to consumers and to the economic underpinning of the Internet.

INTRODUCTION

The cable industry has a long history of protecting the privacy interests of its customers. Long before the advent of broadband Internet service, cable operators operated within the federal

---

[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] "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" ("Green Paper").

privacy regime and cable companies recognize and value their direct relationships with customers.[3] 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 customers. As such, cable companies must take special care with their customers' personally identifiable information ("PII") 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 ("ISPs"), 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.

The appropriate framework for policy discussions is not how to impose the most stringent privacy regime, but rather how to establish policy that encourages continued innovation and evolving technologies while protecting consumers' legitimate privacy interests. NCTA commends the Task Force for its thoughtful policy draft, which recognizes the need to balance the goal of protecting consumer privacy with the objectives of preserving and enhancing innovation on the Internet. Most importantly, we commend the Task Force for recognizing the danger of prescriptive legislation that, by locking in outdated rules, would fail to protect

---

[3] 47 U.S.C. § 551 (Cable Act provision mandating the protection of subscriber privacy).

consumers and stifle innovation.[4] As the Task Force proposes, the most appropriate role for government is to act not as a regulator, but as a coordinator of the process of forging voluntary codes of conduct, and convening interested private and public stakeholders.[5]

The Task Force recommends consideration of a new framework for addressing online privacy issues based on revitalizing certain core privacy principles embodied in Fair Information Practice Principles ("FIPPs").[6] It also envisions flexible implementation of FIPPs and voluntary enforceable codes forged through a multi-stakeholder process in which government convenes industry, academia and policy-makers. NCTA believes this suggested framework is a constructive contribution to evolving privacy policy.

This approach is most likely to ensure protection of consumers' privacy interests while allowing for continued innovation as technologies and business models evolve. In particular, the Task Force rightly recognizes that FIPPs and transparency policies should be implemented in a manner that is tailored to protect privacy without imposing broad-brush restrictions on access to information.[7]

Consistent with the overall approach of the draft report, we urge that the Final Report recognize two additional core principles to ensure an appropriately-tailored privacy framework. *First*, an appropriately tailored privacy framework should distinguish between the risks posed by collection and use of anonymized and aggregated

---

4 Green Paper at 29.

5 *Id.* at 5 (recognizing that the government has a role in the multi-stakeholder approach to play the role of convener – "[i]n this capacity, the government can provide the coordination and encouragement to bring the necessary stakeholders together to examine the innovative new uses of personal information and better understand changing consumer expectations – and identify privacy risks – early in the lifecycle of new products or services.").

6 Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm; Green Paper at 5-6.

7 *Id.* at 5. *Accord* Weitzner, *et al*., Information Accountability, MIT Computer Science and Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2007-034 (June 13, 2007).

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.

Second, competitive neutrality must be included as a bedrock principle of such a framework. Consistent with our view that all consumers and marketplace participants will benefit from a regime of voluntary practices, rather than regulation, parties using functionally similar practices to collect, use, and share covered information should be subject to similar privacy requirements. Imposing different privacy policies based on particular online advertising business models or technologies would disserve consumers and undermine competition in the advertising marketplace.

We also urge the Task Force to reconsider some of its recommendations, which are unnecessary or contrary to the goal of a tailored, competitively neutral framework:

- The Green Paper unwisely dismisses the notice and choice model as a viable means of ensuring consumers make informed decisions about actions impacting their privacy. FIPPS have served long and well as values to guide privacy decision making in a rapidly changing technological and product environment. In addition, they help providers develop flexible privacy options for users that reflect the range of privacy interests within the public.
- The Task Force should more thoroughly examine the degree to which "purpose specification and use limitations" promote the objective of simplifying consumer privacy notices and fostering greater transparency.
- Privacy impact assessments or internal company audits could unnecessarily burden service providers and advertisers without any meaningful consumer benefit. If the Task Force considers such action, it should first seek additional comment and undertake studies about how such mechanisms currently work, their impact on business, and how they should be implemented.
- Enforcement of industry best practices can and should be undertaken by the private sector. Given the well-established track record of industry enforcement of other self-regulatory codes, it is premature to propose FTC or other government enforcement of privacy policies. The ongoing collaborative efforts of industry and government proposed by the Task Force to develop best practices provides a ready forum for ensuring meaningful compliance with those practices.

We look forward to working with the Task Force as it refines its report and helps develop a balanced privacy policy that will serve the interests of consumers and promote continued innovation in services and technologies.

I. THE OVERARCHING PRINCIPLES OF REGULATORY RESTRAINT, RECOGNITION OF THE CONTINUUM OF RISKS AND COMPETITIVE NEUTRALITY SHOULD GOVERN THE INTERNET PRIVACY POLICY FRAMEWORK

There are two important components to establishing an appropriate Internet privacy framework. First, it is necessary to identify and set forth the core principles to be embodied in such a framework. The second step is to identify the best ways to implement those principles. In this section, we discuss three important principles that should be expressly identified in the Final Report.

A. Privacy Guidelines And Policies Should Embrace Regulatory Restraint.

While the Internet inherently presents various privacy issues, those issues should be considered in the context of 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, by definition, 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 Green Paper recognizes one of the potentially adverse consequences of unduly restrictive or overbroad privacy requirements – the threat to online advertising revenues which are the economic underpinnings of Internet content and services. The Task Force recognizes that advertising 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 has been the hallmark of the Internet – and has been a driver of high value jobs that make the U.S. more competitive in the global information market – would surely 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.

In recent years, targeted advertising has begun to play an increasingly large role in supporting the provision of valuable web content and services (often without a fee), fostering innovation on the Internet, and promoting growth and employment in the online services sector.[8] This is because advertising that is more relevant for the consumer is likely to be of greater practical value to the consumer. When online consumers see tailored information about services and offerings that better reflect their interests (based on past purchases or site visits), instead of a barrage of ads that may be of little interest to them,[9] it enables them to make more accurate purchasing decisions in the marketplace. Moreover, targeted advertising is critical for enabling

---

[8] *See e.g.,* Testimony of Joan Gillman, Executive Vice President, Media Sales, Time Warner Cable, Before the House Subcommittee on Commerce, Trade and Consumer Protection, "Do Not Track" Legislation: Is Now the Right Time?, Dec. 2, 2010.

[9] Comments of Computer and Communications Industry Association, Exploring Privacy: A Roundtable Series - Project No. P095416, at 3 (filed Nov. 6, 2009) (noting that consumers are served "relevant ads that are tailored to their online interests").

small online businesses to operate in competition with large websites that have the tools and means to learn much more about their customers.

This type of advertising is not a new concept. Consumer studies and market segmentation are longstanding tools of the advertising trade. For example, magazines frequently insert different ads on the same "page" depending on, for example, location and demographics. Direct mail uses more refined information (such as census data and information collected by third parties) about household interests to customize mailings.

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 are occurring far more 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 an overwhelmingly popular method for advertising because of its effectiveness[10] and its popularity is growing.[11] And although targeted advertising may implicate privacy concerns because advertising can identify consumers that are likely to purchase certain products, the Task Force understands that to the extent these privacy concerns are valid, they must be balanced

---

[10] 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].").

[11] 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 Categorie*s (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.

against the benefits of such advertising in determining whether and to what extent it should be restricted.

NCTA agrees. New regulation could inhibit growth and innovation in the Internet economy and the development of new technologies and services. Prescriptive rules simply cannot keep up with advancement in technology and unique user interests.[12] Given the complexities involved in a rapidly evolving Internet ecosystem, where consumer concerns vary and new services and technologies must respond in these unique contexts, the best approach is one that allows privacy practices and policies to be adapted to evolving technologies in as rapid and flexible a manner as possible.

B. The Final Privacy Framework Should Be Carefully Tailored To Reflect The Continuum of Risks.

The Green Paper's recognition that commercial data privacy policy must address a continuum of risks[13] is a critical – and underappreciated – insight. The debate over online privacy today too often fails to acknowledge that different types of information collection and usage practices create different risks of harm. Any privacy guideline should be carefully tailored to impose restrictions or prescribe practices only where necessary to achieve a legitimate policy goal. Broad restrictions on access and use of data disserve the public by undermining advertiser

---

[12] As NTIA Assistant Secretary Strickling observed: "the rate at which new services develop, and the pace at which users form expectations about acceptable and unacceptable uses of personal information, is measured in weeks or months." Federal agency rulemakings take years and may result in "rules addressing services that may be long abandoned." "*Internet Policy 3.0: All Hands on Deck*", Remarks of Lawrence E. Strickling, Assistant Secretary of Commerce for Communications and Information, Internet Society's INET Series: Internet 2020: the Next Billion Users, April 29, 2010.

[13] Green Paper at Executive Summary ("Commercial data privacy policy must address a continuum of risks to personal privacy, ranging from minor nuisances and unfair surprises, to disclosure of sensitive information in violation of individual rights, injury or discrimination based on sensitive personal attributes that are improperly disclosed, actions and decisions in response to misleading or inaccurate information, and costly and potentially life-disrupting identity theft."); *id.* 39, n.114 ("As noted at the beginning of our report, commercial data privacy policy must cover a continuum of harms, ranging from minor nuisances to identity theft and other forms of economic harm.").

supported content and services.

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, or 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.

The collection and use of information on an aggregated or anonymized basis simply does not compromise the privacy of an individual and need not be subject to the kind of restrictions appropriately accorded to the collection and use of individual and identifiable information. While some fear that anonymized, aggregate data can be readily and easily reverse-engineered, these concerns are based on a few anomalous Internet experiences in which anonymization techniques were poorly executed. That there are a few such examples, however, does 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.

While there is a risk that aggregated or anonymized data could be reverse engineered so as to identify an individual, there are readily available techniques to reduce such risk, such as encryption and hashing techniques that are continually being improved. Other federal agencies

are increasingly recognizing such techniques as effective in protecting personalized data.[14] The Task Force should consider seeking input from NIST on the capabilities of encryption technologies as a means of safeguarding personal information. 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. At the very least, the Final Report should insist that any policies favored do not have the perverse effect of discouraging privacy-enhancing techniques that would benefit consumers.

C. Privacy Guidelines And Policies Should Ensure Competitive Neutrality.

As it considers its recommendations for privacy guidelines and policies, the Task Force 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 characterized by rapid technological change such as online advertising, 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

---

[14] *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), 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).

participants into one sanctioned approach. Moreover, limiting online advertising to specified designated permissible techniques would deter new entry, and limit competition.

The different entities involved in online behavioral advertising should not be subject 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. In the context of global interoperability, the Green Paper recognizes that "[d]isparate approaches to commercial data privacy can create barriers to both trade and commerce, harming both consumers and companies."[15] The same concern applies here. The Task Force 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, 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 Green Paper does not cite to 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

---

[15] Green Paper at 53.

or approach, provided that it offers the necessary security and privacy for consumers. Accordingly, the Task Force should focus on the permissible use of data, not which technology is used to collect and store it, and the final 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.

In the evolving Internet marketplace, competition extends across the multiplicity of categories of service providers. Cable operators compete, of course, with other providers of broadband Internet access service, 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* that affects the privacy interests of consumers and do not single out particular categories of service *providers* for special treatment. 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.

II. THE GOVERNMENT SHOULD IMPLEMENT THE PRIVACY FRAMEWORK THROUGH INDUSTRY SELF-REGULATION INFORMED BY EVOLVING CONCEPTS AND INITIATIVES AND OTHER POLICIES CONSISTENT WITH OVERRIDING PRINCIPLES

With the overarching principles firmly in place, policy-makers can determine how best to implement them. A corollary of the core principle of regulatory restraint is that it is impossible to identify in advance a comprehensive set of rules and regulation that will accommodate the need for flexibility in anticipating and dealing with evolving Internet privacy issues. This means that a voluntary self-regulatory approach is far superior to any comprehensive government rules

and enforcement. Within that self-regulatory approach, it is possible to identify certain proposals that will – or will not – further the overriding principles of privacy policy.

A. The Final Report Should Recommend A Voluntary, Self-Regulatory Approach To The Development Of FIPPS.

NCTA generally supports the idea of developing "voluntary, enforceable codes of conduct that allow for continued flexibility as technologies and business models evolve" which would "disfavor prescriptive rules" and promote innovation and the "free flow of goods and services online."[16] Voluntary FIPPs represent a potentially promising approach, as long as they preserve flexibility and allow for the development of tailored implementation plans that correspond to the privacy risks posed by their services and allow consumer privacy protection to adapt as new technologies emerge.

1. Implemented flexibly, FIPPs can be an important part of effective privacy policy.

NCTA agrees that FIPPs should "promote informed consent without imposing undue burdens on commerce and on commercial actors"[17] and that certain FIPPs could be "highly effective in increasing consumer understanding of commercial data practices while remaining a flexible, low-cost legal framework."[18]

A FIPPS framework that promotes the development of robust voluntary codes of conduct should build upon the privacy protection tools that 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 commenting parties agree that the various tools currently being offered and in development will more fully engage consumers in their privacy choices and give them the ability

---

[16] Green Paper at 4.

[17] *Id.*

[18] *Id.* at 34.

to control their choices.[19] As the Task Force notes, for example, there are new privacy-enhancing technologies and 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.[20] This approach would also allow industry self-regulatory initiatives to continue to evolve, informed by the ideas and recommendations to be issued in the Final Report. Using current industry initiatives as a baseline for the development of FIPPs also would ensure that FIPPs processes and policies are developed and applied in a competitively and technologically-neutral fashion.

The proposed Privacy Policy Office may be an ideal forum in which to convene collaborative efforts to develop best practices for industry self-regulation.[21] As the Green Paper suggests, there are substantial benefits to having a uniform policy for online privacy.[22] The Privacy Policy Office could diminish the risks and disadvantages associated with today's disparate state privacy policies by facilitating the adoption of more consistent voluntary FIPPs and uniform application of voluntary policies.

In contrast, seeking to implement FIPPS via statute or administrative rules would be the lengthiest and likely least effective manner of addressing current privacy concerns. As the Green Paper recognizes, privacy issues are constantly evolving and statutory or regulatory-based FIPPs would likely be outdated before they are even adopted.[23] Moreover, it would be highly

---

[19] *Id.* at 45-46 (recognizing that "a number of commenters noted that privacy- by-design and technological approaches, such as icons on advertisements or profile management dashboards, could be used to implement industry standards"); *see also id.* at 146, n.125 (summarizing such comments).

[20] Green Paper at 34 (discussing the initiative by online advertisers to launch "an 'enhanced notice' campaign to present more information about ads in the context in which ads are viewed.").

[21] *Id.* 45-46.

[22] *Id.* at 68.

[23] *Id.* at 29 (recognizing that "the downsides" expressed by commenters that legislation would "lock[]-in outdated rules that would fail to protect consumers and stifle innovation.").

impractical to attempt to create statutory or administrative rules that could effectively include the wide range of services and businesses that a FIPPs framework could potentially address.[24]

Instead, the Task Force should encourage the development of FIPPs, new technologies and policies through industry working groups. Working with industry experts should be essential in determining if a new idea, such as "Do Not Track," is even viable in the online marketplace.[25] In doing so, the Task Force would confirm the Green Paper's recognition that government must work with industry stakeholders to "examine the innovative new uses of personal information and better understand changing consumer expectations – and identify privacy risks – early in the lifecycle of new products or services."[26] Adopting this approach with the Report's general recommendation that government not necessarily act as a regulator, but rather as a convener of industry, academic and public stakeholders, is the best policy.

2. The development of FIPPs and other privacy policies should take into account existing self-regulatory initiatives.

In a highly volatile, highly competitive online marketplace, there is strong reason for the government to restrain regulatory impulses and to strive for an industry-driven self-regulatory approach. As the Green Paper acknowledges,[27] cable ISPs 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 FTC and other agencies, entities interested in online advertising have advanced a

---

[24] *Id.* at 32 (noting that the "range of services, business models, and organization structures to which a FIPPs-based framework would apply counsel against attempting to develop comprehensive, prescriptive rules.").

[25] *See* Testimony of Daniel J. Weitzner, Associate Administrator for Policy Analysis and Development, NTIA, before U.S. House Subcommittee on Commerce, Trade and Consumer Protection, "Do Not Track Legislation: Is Now the Right Time?, December 2, 2010 (in advocating a dynamic multi-stakeholder process for Do Not Track proposals.

[26] Green Paper at 5.

[27] *Id.* at 28.

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. The Green Paper discusses one such initiative, noting the industry's 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.[28] In addition to the efforts recognized by the Green Paper, 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; Mozilla's Firefox browser offers plug-ins for opt-out,[29] 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.[30]

Since the 1984 Cable Act, the cable industry has adopted and incorporated FIPPs into everyday practices. Today many cable companies have internal data governance and management structures in place to protect consumer data and ensure the proper use of PII. Such companies also consider privacy concerns in every aspect of their business, including product design, implementation of accountable business practices, and the creation of strong security measures. Privacy and security controls related to cable broadband access have become standard

---

[28] *Id.* at 28, 34.

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

[30] *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.").

practice in protecting consumers from malware, spyware, viruses and other privacy invasions. In short, the industry – as a whole – has been actively creating privacy mechanisms to meet the needs of its consumers. Moreover, there is extensive involvement by all players in the online advertising market in privacy coalitions and self-regulatory bodies.

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. Indeed, online advertising provides the foundation to support the "hallmark of the digital economy" which "is the wide variety of rapidly evolving products, services, and content that are often made available free of charge in part through the use of personal data"[31] obtained through online marketing. As the Task Force and other commenting parties acknowledge, online advertising not only supports valuable content on the web (often without a fee), but is the key to fostering jobs, growth and innovation in online services.[32]

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. The Final Report's recommendations for privacy guidelines should take into account the existing and anticipated efforts to refine and expand self-regulatory mechanisms that will protect consumer privacy while preserving and enhancing the benefits that

---

[31] Green Paper at 32 citing to the Daltran comment which noted that "online marketers . . . subsidize free content on the Internet.").

[32] *Id.* at 14 (noting that "according to one estimate, as of 2009, advertising-supported Internet services directly or indirectly employed three million Americans"); *id.* at 19, n.53 (citing the Advertising Agencies Comment at 1 ("The revenue generated by online advertising supports the creation and entry of new businesses, communication channels (*e.g.*, micro-blogging sites and social networks), and free or low-cost services and products (*e.g.*, email, photo sharing sites, weather, news, and entertainment media.").

online advertising creates for the entire Internet community.[33] The cable industry welcomes the opportunity to work with the Task Force on these issues and to update it on the development of industry self-regulatory mechanisms and specific company efforts.

Whatever framework is adopted, however, due regard must be given to Federal sectoral laws and policies.[34] As the Green Paper notes,[35] cable operators have long been subject to a privacy framework under the Cable Act that has provided cable subscribers with strong privacy protection for more than 25 years (as well as customer proprietary network information (CPNI) rules for Voice over Internet services). Whether this framework is also appropriate for cable operators' ISP business, or whether the better approach is to ensure uniform treatment of all ISPs, is a matter for continued discussion.

Similarly, contrary to the Task Force's suggestion, once any federal framework is adopted, it should explicitly preempt state privacy laws.[36] As commenting parties have noted, national consistency would make compliance simpler for businesses, and could help consumers better understand what privacy protections cover their information on the Internet.[37] Allowing states to continue to create a patchwork of regulations would be unworkable and inconsistent with the push towards a federal baseline privacy framework, as well as inconsistent with the tailored and restrained regime NCTA advocates. Indeed, due to the national, and often

---

[33] *Id*. at 32 (noting that "Commenters . . . cautioned against policies that would alter the existing economic balance.").

[34] *Id*. at 58.

[35] *Id.* at 11 (noting, in general, that the U.S. "protects personal data through a sectoral framework that has facilitated innovation and spurred some of the world's most technologically advanced services, while also providing meaningful privacy protections").

[36] *Id*. at 61 (recommending that any "new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.").

[37] *Id*. This is true for cable privacy as well, although current law permits states and localities to adopt privacy requirements in addition to those established in the Federal Cable Act. 47 U.S.C. § 551(g).

international, nature of the businesses and equipment markets, Federal law frequently preempts state and local laws in this area, especially in matters of technology design. A web site should not have to appear to viewers in different ways depending on the state they are in.

Enforcement of privacy policies through private rights of action – particularly for class action lawsuits[38] – 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 foster innovation in the online behavioral advertising marketplace, as well as to promote competitive entry for ISPs and others, the Final Report should

---

[38] *Id.* at 29 (noting that "there was disagreement on the role for private rights of action in such a framework"). The Cable Act also permits private rights of action to enforce violations of the cable privacy provisions. That aspect of cable privacy policy should also be reformed.

recommend the creation of a competitively neutral "safe harbor" status to all companies adhering to self-regulatory principles developed under the FIPPS. Such an approach will help promote innovation in products, services and in protection of personal privacy, as well as support the creation of jobs in this important area of our economy.

B. Absent Empirical Evidence of Harm That Justifies Greater Government Intervention, Enforcement Provisions Are Unnecessary.

The Green Paper proposes a regime of voluntary enforceable codes of conduct in which such codes would address emerging technologies and issues not covered under current baseline FIPPs. It proposes various incentives for stakeholders to develop such codes, including greater engagement by Executive branch officials and the Federal Trade Commission ("FTC") to encourage industry-led efforts, increasing the level of FTC enforcement under current law, or legislation to create a safe harbor for companies that commit and adhere to an appropriate voluntary code of conduct.

For all of the foregoing reasons, NCTA supports industry self-regulation with greater government engagement as a convener, not a regulator. Absent evidence of chronic and purposeful violations of industry best practices or standards, government enforcement provisions are premature. Enforcement of industry best practices can and should be undertaken by the private sector, as occurs with other industry self-regulatory bodies (for example, sports leagues and engineering bodies). The record and the rationale cited in the Green Paper do not support the adoption of any government enforcement mechanisms at this time for any voluntary FIPPS adopted.

If government enforcement proves necessary, the FTC would be the appropriate agency to undertake that role. But, at least for now, Congress should first be given a chance to define the range of acceptable activities, with agency enforcement defining their scope only if

experience proves it necessary.

C. Enhanced Transparency Mechanisms Should Account For Current Industry Practices And Should Be Tailored To Specific Consumer Interactions.

NCTA's members share the Task Force's belief that "maintaining consumer trust is vital to the success of the digital economy,"[39] and support the objective of making customer choice on privacy issues simpler and easier through providing more transparency, provided that any policy is appropriately restrained 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. In devising recommendations for mechanisms to provide comprehensive yet simplified choice options, however, the Task Force should take several important considerations into account.

First, while NCTA agrees that there are "commonly accepted practices" for which no consent need be obtained, attempting to create 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. Any concept of "commonly accepted practices" must be based on clear principles and allow for those practices to evolve over time as customer familiarity and exposure evolves, without the need to add specific amendments to the list. Consumers could be educated about the *kinds* of uses to which their data may be subject, rather

[39] Green Paper at 15.

than every possible such use.[40] Calling such practices "legitimate business practices" may more accurately convey this goal.[41]

More generally, any such practices should include the collection of information when it is not 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.

Second, efforts to create greater clarity and consumer-friendly notice regarding the collection and use of information should avoid 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. Recommendations can be more readily and effectively implemented in a framework of regulatory restraint that offers flexibility for innovation and experimentation, than via "one size fits all" regulatory mandates. This approach would also allow companies to use more creative educational tools to educate the public, such as online videos, VOD training, live Q&A sessions, or other means. 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 operator being subject to multiple, potentially conflicting and duplicative disclosure obligations. This would be unfair to cable operators and highly confusing to their subscribers.

---

[40] 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).

[41] 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.

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. A regulatory regime where routine activities such as opening a web page or clicking on a link result 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.

D. The Final Report Should Not Dismiss Notice And Choice As A Viable Approach.

The Green Paper dismisses the notice and choice model as a viable means of ensuring consumers make informed decisions about actions impacting their privacy.[42] Although the Green Paper notes that there are concerns about the notice-and-choice model when the "relevant notice is not transparent," and cites to the use of legalese in such notices,[43] 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, and consumers are not seeking new or different notifications concerning these types of practices. Moreover, the paper acknowledges that criticism of notice-and-choice was not uniform and that

---

[42] *See, e.g.*, Green Paper at 32 (asserting without support that the "current privacy policy framework provides consumers with a limited basis to understand the basis of [an] economic bargain").

[43] *Id.* at 31.

it does meet today's marketing needs.[44] Given these conclusions, the Task Force should acknowledge explicitly that notice and choice remains a viable model for addressing consumer privacy.

E. Purpose Specifications And Use Limitations Are Unnecessary At This Time And Could Hinder Innovation.

While simplifying consumer privacy notices and fostering greater transparency represent sensible policy objectives, the Task Force should more thoroughly examine the degree to which "purpose specification and use limitations" promote those objectives. As currently described,[45] the "purpose specifications and use limitations" seemingly offer nothing more than an additional layer of notification, the need for which clear and transparent notice requirements will likely already address. As such, they appear unnecessary.

The Task Force apparently fears that an "entity that clearly states that it intends to do anything and everything with the data it collects may be transparent, but may not be providing adequate protection for consumer privacy."[46] However, its proposed solution – requiring companies to "provide clear notice of their practices" and prohibiting companies from "deviating from the purposes and uses to which they commit"[47] – would likely create a system where companies would need to send frequent updated notices concerning the use of data which would confuse customers and perhaps cause unnecessary alarm. Prohibiting companies from deviating from initial uses would also hinder the development of innovative technologies.

Additionally, it is unclear that consumers even face any harm by secondary uses of their

---

[44] *Id.* at 27 (noting that "some commenters voiced explicit support for this framework").

[45] *Id.* at 37-39.

[46] *Id.* at 38.

[47] *Id.*

personal data,[48] which could render this potentially confusing and burdensome requirement useless. Rather than endorse rigid purpose specification and use limitations, the Task Force should encourage industry to address in the FIPPS process the most effective approaches and mechanisms to evolving privacy policies and notices to address new uses and practices.

F. Privacy Impact Assessments And Audits Are Unnecessary To Ensure Compliance With FIPPs.

There is no evidence in the record to support a full-fledged endorsement of privacy impact assessments ("PIAs") or internal company audits. And while privacy impact assessments are common among governmental organizations, no government has mandated a privacy impact assessment for business.[49] The Final Report should instead recognize that these tools – PIAs and audits – are just two of many different possible accountability mechanisms aimed at fostering and ensuring companies' fidelity to their information policy principles and practices. For example, the privacy by design concept endorsed in the FTC Report represents a helpful and innovative approach that could effectively integrate from the outset of the design, development and provisioning of a new service many of the safeguards and objectives designed to be achieved through audits or PIAs.

As such, the Final Report should endorse flexibility and innovation in the creation of accountability mechanisms designed to promote adherence to industry privacy policies and

---

[48] *Targeted Online Advertising: What's the Harm & Where Are We Heading?, Berin Szoka & Adam Thierer, Progress on Point*, The Progress & Freedom Foundation, Vol. 16, Issue 2, at 4 (June 2009) (noting, with respect the secondary uses of online behavioral information, that the "FTC itself notes that 'such uses do not appear to be well-documented.'").

[49] *See* Privacy Impact Studies: An International Study of their Applications and Effects, Loughborough University, October, 2007 page 13 *at* http://docs.google.com/viewer?a=v&q=cache:g9eoyAW5K0wJ:www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf+%22privacy+impactassessment%22+study&hl=en&gl=us&pid=bl&srcid=ADGEESgRQsUvQoZUM56YXSUVP0GdALTAJ8STlQmRqEjx0pXUPO5wANt5gJjb4OyAt40nR_mtzXJy-KNMjCdO18ie5c3HTDWIBb6qhgkxAYxm7SmDm5QaKb13Kbvav67QI6szoPX9ZmbH&sig=AHIEtbRm3bHSRNAWS9G4AQlyjDDL06yCpQ.

should not, as currently drafted, adopt either mechanism until further research is done. For instance, the Green Paper broadly calls for the adoption of PIAs as a mechanism to enhance transparency.[50] However, it does not offer evidence that PIAs would actually facilitate consumer understanding and transparency. Rather than recommend a full-scale adoption of PIAs across various industries and business models, the Final Report should recommend further investigation of this type of mechanism. Likewise, the Task Force should refrain from adopting mandatory audits until there is evidence of widescale non-compliance.[51] No such evidence is provided in the draft; the Green Paper cites a single commenter to support its call for a robust auditing requirement and broadly asserts that audits are a foundation to building consumer trust.[52] Like NCTA's proposed approach to PIAs, the Final Report should recommend further investigation of the types of audits and benefits that may accrue from them before recommending a final course of action.

---

[50] Green Paper at 34.

[51] *Id.* at 40.

[52] *Id.*

CONCLUSION

In a constantly-evolving online environment with many new technologies and services, the Task Force has appropriately recognized that privacy policy must protect individuals without sacrificing the innovations, choice, and new content options that the accountable use of information makes possible. That policy is best implemented through a framework that relies in the first instance on self-regulation, with input and greater engagement between government and industry stakeholders (through the proposed Privacy Policy Office).

Cable operators have a strong commercial interest in protecting privacy and building trust with consumers, rendering much regulation unnecessary except when specifically tailored to address identified substantiated risks. The Final Report should advocate strongly for a more comprehensive and balanced assessment of the costs and benefits of policies that would restrain online advertising in the name of promoting privacy.

Respectfully submitted,

/s/ Rick Chessen

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

January 28, 2011