Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51

COMMENTS OF THE FUTURE OF PRIVACY FORUM

Christopher Wolf
Co-Chairman
Jules Polonetsky
Co-Chairman and Director
THE FUTURE OF PRIVACY FORUM
919 18th Street, NW
Washington, DC 20036
www.futureofprivacy.org

Christopher Wolf
Mark W. Brennan
Sarah P. Reisert
HOGAN AND HARTSON
555 13th Street, NW
Washington, DC 20004
(202) 637-8834
Facsimile: (202) 637-5910
E-mail: cwolf@hhlaw.com
Counsel for THE FUTURE OF PRIVACY FORUM

June 8, 2009

TABLE OF CONTENTS

Page

Executive Summary i

I. Introduction 2

II. About the Future of Privacy Forum 3

III. Broadband Use Implicates Personal Privacy 3

A. The Collection, Use, Sharing, Security, and Disposal of Personal Information Occurs at Many Places on the Internet. 4

B. Current Data Sharing and Collection Practices Raise Privacy Concerns 7

1. Consumers Do Not Always Fully Understand or Are Not Able to Control Adequately Data Collection Practices. 7

2. The Collection of Consumer's Personal Data Also Raises Invasion of Privacy, Identity Theft, and Discrimination Concerns. 8

IV. To Safeguard Consumers and Promote Broadband Adoption and Use, the Commission Should Ensure that its National Broadband Plan Addresses the Critical Privacy Elements of Transparency and Control 11

A. Companies Should Recognize That They Have an Ongoing Relationship with Their Customers and Should Focus on Improving Transparency and Control. 11

B. FPF is Working to Advance Transparency and Consumer Control. 14

C. Internet Companies Should Help Provide Privacy Solutions. 16

V. A Mix of Government Oversight of Privacy and Data Security and Self-Regulation are Beginning to Drive Improved Industry Practices 17

A. Privacy and Data Security Issues Implicated by Widespread Broadband Use are Receiving Significant Attention From Federal, State, and International Government Bodies. 17

1. FTC Report: Self-Regulatory Principles for Online Behavioral Advertising (February 2009). 17

2. FTC Mobile Marketing Report (April 2009). 18

TABLE OF CONTENTS—Continued

Page

3. Congress. 19

4. States. 20

5. International. 22

a. European Union. 22

b. Canada. 23

B. Industry Members are Continuing to Develop Leading Practices for Nascent Broadband Technologies, Consistent with the FTC's Guidance and Other Incentives. 23

1. The Network Advertising Initiative. 24

2. TRUSTe. 25

3. Interactive Advertising Bureau. 26

4. The Mobile Marketing Association. 27

5. CTIA – The Wireless Association. 28

VI. Conclusion 29

EXECUTIVE SUMMARY

Concern for privacy and respect for user information should be an integral part of the national broadband plan the Commission is formulating. Privacy means that consumers are meaningfully informed about and have control over how those offering Internet services — services that are optimized through the use of broadband facilities — collect and use personal data. Only if consumers have confidence about how their data is used will there be the growth in Internet services that is essential to a national broadband plan.

Today, many consumers do not fully understand how their information, whether anonymous or identifiable, is being used by those providing Internet services. The technologies used for online tracking of consumer activity (and involving the collection of user data) are not always disclosed to or readily understood by the consumer. Often, privacy policies and similar disclosure mechanisms are unclear and lead to consumer confusion.

The national broadband plan should make clear that transparency and control are essential to consumers' confidence about the privacy of their information online, and that only with such consumer confidence will we achieve the Internet usage that is tied to our national broadband goals. Internet companies operating under the national broadband plan must recognize that they have an ongoing relationship with their customers and that continued trust from customers is critical to maintaining that relationship, and to growing Internet business. Such trust can only be achieved if consumers feel that they are receiving sufficient information about and are in control of how their personal data is used online.

Thus, when Internet companies offer customized online experiences through the collection and use of user data, or participate in targeted online advertising, they must make clear to consumers what is happening and must give consumers real choice over the collection and use

of their data for such activities. In addition, if a consumer elects not to have personal information collected or shared, companies must respect that decision in an enforceable manner.

Ongoing government oversight of privacy and data security issues in the United States and abroad demonstrates a growing consensus in support of transparency and consumer control. In addition, Internet companies are developing best practices designed to promote transparency and control and protect consumer privacy and data security. These organizations, including The Future of Privacy Forum, are committed to advancing privacy practices to promote consumer confidence. The Commission should take the current regulatory and self-regulatory framework into account as it develops a national broadband plan that includes privacy as an essential component.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51

COMMENTS OF THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum ("FPF") hereby submits its Comments in response to the Federal Communications Commission's ("FCC" or "Commission") April 8, 2009 Notice of Inquiry ("*NOI*") in the above-referenced proceeding.[1] Pursuant to the American Recovery and Reinvestment Act of 2009,[2] the Commission is to submit to Congress a national broadband plan that ensures that every American has access to broadband capability and establishes clear benchmarks for meeting that goal. As described below, privacy should be an integral part of the national broadband plan the Commission is formulating. Privacy means that consumers are informed about and have control over how those offering Internet services (optimized through the use of broadband facilities) collect and use personal data. Only if consumers have confidence about their privacy will there be the growth in Internet services that is essential to a national broadband plan.

[1] *A National Broadband Plan for Our Future*, GN Docket No. 09-51, Notice of Inquiry, FCC 09-31 (rel. Apr. 8, 2009) ("*NOI*").
[2] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) ("Recovery Act").

I. Introduction

In the *NOI*, the Commission seeks comment on a range of privacy issues related to broadband use.[3] In particular, the Commission seeks comment regarding consumers' expectations of privacy when using broadband services or technologies and whether privacy concerns have an impact on broadband adoption and use.[4] It also asks how the Commission should treat issues such as deep packet inspection ("DPI") and behavioral advertising, and whether these or other practices "discourage consumers from 'access[ing] the lawful Internet content of their choice' for fear of having that access tracked or revealed."[5] The Commission also seeks comment on the role that privacy protections play in enhancing consumer welfare[6] and whether the protection of customers' private information would spur consumer demand for and adoption of broadband connections.[7]

The Commission is entirely correct to consider the privacy issues related to broadband use as part of its national broadband plan, as reflected in the *NOI*. The collection, use, sharing, security, and disposal of personal information occurs at many places on the Internet and often involves numerous parties. These activities create risks to consumers such as identity theft and raise concerns over unwanted publicity of personal information to unintended recipients. It is axiomatic that consumers only will expand their adoption and usage of broadband services and technologies if they can be confident that there are adequate privacy and data security protections available.

To safeguard consumers, the Commission should specify in its national broadband plan the importance of two critical privacy elements—transparency and control. The Commission

[3] *NOI* ¶¶ 58-60.
[4] *Id.* ¶¶ 52, 59.
[5] *Id.*, citing *Internet Policy Statement*, 20 FCC Rcd 14986, 14988 ¶ 4 (2005).
[6] *Id.* ¶ 66.
[7] *Id.* ¶ 59.

should also underscore the importance of the ongoing government oversight of privacy and data security practices, including transparency and control, as it develops the national broadband plan. Leading industry practices, moreover, are evolving to provide enhanced transparency and control to consumers, and these self-regulatory practices should be taken into account as the Commission seeks to encourage the greater adoption and use of broadband services and technologies.

II. About the Future of Privacy Forum

Founded in 2008, FPF seeks to improve online privacy through responsible data practices. Specifically, among its other efforts, FPF advocates greater transparency about the collection and use of personal data by online businesses, along with greater user control over such collection and use. Supported by AOL, AT&T, Deloitte, eBay, Facebook, Intel, The Nielsen Company, TRUSTe, Verizon, and Yahoo!, and with an advisory board of leading privacy advocates from business, law, NGOs and academia,[8] FPF seeks to identify and develop leading practices regarding the way consumers are informed about personal data collection and use online, and how consumers can exercise control over such collection and use.

III. Broadband Use Implicates Personal Privacy

As the Commission acknowledges in the *NOI*, "Americans are using broadband to perform everyday tasks in which they pass personal and confidential information over broadband connections, raising important consumer privacy concerns."[9] Today, consumers access the Internet to pay bills; maintain bank accounts; file taxes; communicate via e-mail, blogs, instant messaging, and social networking sites; purchase clothing, household goods, and entertainment

[8] About the Forum, http://www.futureofprivacy.org/2008/11/10/about-the-forum/ (last accessed June 8, 2009). Supporters and advisory board members are not responsible for positions taken by FPF.
[9] *NOI* ¶ 58.

items; read newspapers; conduct research on personal issues, including politics, legal matters, health and welfare, and finances; and receive remote healthcare monitoring.[10]

In addition to streamlining consumers' lives, the use of these convenient services and applications also produces secondary benefits that enhance consumers' online experience. Through the collection of consumer data, companies provide users with customized online experiences through personalized content and targeted advertisements. When provided with appropriate transparency and control, such personalization can be relevant and responsive to consumers' needs, generate increased business revenues, and subsidize free online content.[11] With the development of nationwide broadband availability, companies will have additional opportunities to develop new business models, improve data collection technologies, create new services and applications, and personalize consumer content further. Along with these benefits from advanced data sharing, however, come significant challenges. The changing marketplace will encourage businesses to delve more deeply into data that can be used to make more efficient and effective marketing decisions.[12] Moreover, the attendant risks of data sharing not only raise questions regarding how companies will continue to collect, combine, and disclose consumer data, but also raise critical consumer privacy concerns.

A. The Collection, Use, Sharing, Security, and Disposal of Personal Information Occurs at Many Places on the Internet.

As recently explained in a TRUSTe report, the collection, use, sharing, and disposal of consumers' personal information occurs online at the many Web sites that consumers visit on a

[10] *See id.* ¶ 58, n. 85; *see also* Jordan McCollum, *Study Looks at Internet Use in America*, WEBPRONEWS, Jan. 2, 2008, http://www.webpronews.com/topnews/2008/01/02/study-looks-at-internet-use-in-america (last accessed June 8, 2009).
[11] *See* Future of Privacy Forum Mission, http://www.futureofprivacy.org/2008/11/15/the-future-of-privacy/ (last accessed June 8, 2009).
[12] *Id.*

regular basis.[13] Such data collections are not only used by those Web sites, but are also shared with a variety of third parties, including but not limited to vendors, intermediaries, content providers, ad networks, affiliates, exchanges, and data analytic firms.[14] These parties also collect and share non-personally identifiable information related to consumers by tracking their online activity. To carry out these first-party data collection and third-party data sharing activities, companies rely on users' IP addresses, cookie IDs, ad tags, pixel tags, Web beacons, account IDs corresponding to registered users, log files, and other data.[15] Generally, these technologies permit companies to either recognize the user's browser or direct a user's browser to present itself to servers so data about the user's online activity at one site or across many Web sites can be used or personalized content and advertisements can be delivered.[16]

Behavioral advertising is a contemporary example of personal data collection through such technologies and how anonymous information can be used to tailor advertising and marketing messages. According to the Federal Trade Commission ("FTC"), "[o]nline behavioral advertising involves the tracking of consumers' online activities in order to deliver tailored advertising. The practice, which is typically invisible to consumers, allows businesses to align their ads more closely to the inferred interests of their audience."[17]

One such example of online tracking includes companies' use of cookies placed on the consumer's computer. Upon researching hotels in Las Vegas, the Web site viewed by a user

---

[13] TRUSTe, *Online Behavioral Advertising: A Checklist of Practices that Impact Consumer Trust*, 4 (Feb. 2009) ("TRUSTe Whitepaper"), *available at* http://www.truste.org/pdf/Online_Behavioral_Advertising.pdf.
[14] *Id.*
[15] *Id.* at 12-13 (describing the technological tools Web sites and third parties employ to collect and transfer data originating from the consumer's Web activity and ending with the ad network, data analytics firm, or the like).
[16] *Id.*
[17] Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising*, 2 (Feb. 2009) ("FTC Principles"); *see also* TRUSTe Whitepaper at 5-7 (outlining that the spectrum of behavioral uses includes tailoring advertisements on a Web site to a certain consumer or consumer groups, tailoring advertisements across Web sites commonly owned by a company, providing data to an ad server to target advertisements for a specific publisher, tracking for analytics research, and making data available to third parties via an ad exchange for unlimited use or to an ad network for use on other sites).

displays banner advertisements for a local hotel. Here, the Web site or third party ad network recognized the unique cookie on the consumer's Web browser, which enabled the data collector to correlate data about Web sites visited, banners clicked on, or search terms entered at other sites in its network.[18]

The collection of consumers' personal data for the purposes of behavioral advertising also can be used in conjunction with other forms of targeting based on factors like geography, demographics, the surrounding content, or offline information. Activities such as data mining, so-called DPI advertising, consumer profiling, and location-based tracking through mobile devices allow companies to take advantage of consumers' personally identifiable and non-identifiable information (respectively, "PII" and "non-PII") to provide commercial information to them. While the information gathered by advertising networks is often not explicitly personal, consumers' online activities across Web sites can be combined to create consumer profiles. Moreover, consumers' location-based information derived from their mobile devices may reveal sensitive information relating to visits to a doctor, government agency, or other establishments.[19] The FTC and advocates have observed that such profiles can then be intentionally or inadvertently linked with offline data or with PII as a URL string automatically transmits it through a cookie or Web sites provide that information directly to network advertisers (*e.g.*, the demographic information supplied to register for a free e-mail account is combined with user search data).[20]

---

[18] *See* FTC Principles at 2 (describing how a network advertiser places and uses a cookie on a consumer's computer to deliver targeted advertisements).

[19] Federal Trade Commission, *FTC Staff Report: Beyond Voice – Mapping the Mobile Market Place*, 17 (Apr. 2009) ("FTC Mobile Marketing Report").

[20] Federal Trade Commission, *Online Profiling: A Report to Congress*, 7-8 (June 2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf; *see also* Center for Digital Democracy and US Public Interest Research Group, *Supplemental Statement in Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices*, FTC Town Hall "Ehavioral

B. Current Data Sharing and Collection Practices Raise Privacy Concerns

1. Consumers Do Not Always Fully Understand or Are Not Able to Control Adequately Data Collection Practices.

Although many consumers may appreciate a personalized online experience provided by behavioral advertising and other online data collection processes, there are privacy issues that must be navigated to offer users this experience responsibly. According to FTC Commissioner Pamela Jones Harbour, "[m]ost consumers do not fully understand the types and amount of information collected by businesses, or why the information may be commercially valuable. To the extent that the industry currently attempts to provide notice and choice to consumers, such efforts are insufficient."[21]

In practice, many Web site privacy policies are not easily understood and have the potential for consumer confusion.[22] Moreover, the variety of technologies used for online tracking are not always disclosed to or readily understood by the consumer. Consequently, consumers are not fully informed as to who is collecting the data, cannot see all the information that is being collected about them, and they do not have the ability to access or control the profiles that marketers have compiled.[23] FTC Commissioner Harbour has noted that consumers do not realize that, often, this data cannot simply be recalled, rectified, or deleted.[24] TRUSTe has stated that this lack of awareness is troublesome because the aggregation of online

---

Advertising: Tracking, Targeting, and Technology," 38 (filed Nov. 12, 2007) ("CDD/PIRG Supplement"), *available at* http://www.ftc.gov/os/comments/behavioraladvertising/071112cdduspirg.pdf.

[21] Press Release, Future of Privacy Forum, Future of Privacy Forum Announces Research Initiative to Develop Effective Messages to Communicate with Users About Online Data Use (May 19, 2009) ("FPF Research Initiative"), *available at* http://www.futureofprivacy.org/2009/05/19/future-of-privacy-forum-announces-research-initiative-to-develop-effective-messages-to-communicate-with-users-about-online-data-use/.

[22] As discussed in Section IV(A) below, the current practice of notifying consumers of data collection practices and opt-out policies through a Web site's privacy policy is often ineffective because these lengthy, jargon-filled policies are not easily understood by consumers and the opt-out procedures are difficult to locate in the document or located on a third party Web site.

[23] *See* FTC Principles at 30-37; FTC Principles, Concurring Statement of Commissioner Pamela Jones Harbour, 3-4 (Feb. 2009) ("Harbour Statement").

[24] *See* Harbour Statement at 1.

information culled from different services and systems reveals patterns and trends that allow the data collector to know more about the consumer than the consumer might expect (and that could possibly identify the individual consumer). As Internet advertising continues to evolve, consumer confusion regarding data flow and its ultimate use could continue.[25]

2. The Collection of Consumer's Personal Data Also Raises Invasion of Privacy, Identity Theft, and Discrimination Concerns.

There is also a concern that sensitive information regarding health, finances, certain demographics, or children could fall into the "wrong hands or be used for unanticipated purposes."[26] Because data collection often remains invisible to the user, consumers may believe that certain online activity — researching diseases, purchasing medications, reviewing mortgage options, tracking stock quotes, exchanging financial information, or updating profiles on social network sites — is anonymous.[27] However, when such information is aggregated and linked by a common identifier, the resultant "highly detailed and sensitive profile" can be traced to the consumer or combined with "even richer, more sensitive, data" to identify that consumer, or it can fall into the wrong hands and be used against the consumer for unlawful or discriminatory purposes.[28] Although some individual companies or self-regulatory groups have guidelines against sensitive uses of profile data, it is also the case that some of these policies are overly-general, ambiguous, or are not publicly available.

Through a recent survey, TRUSTe learned that 51 percent of consumer respondents worry about protecting their private information online.[29] The survey indicates that 75 percent of consumers "say they know how to protect their personal information online, yet 39 percent admit

[25] TRUSTe Whitepaper at 3.
[26] FTC Principles at ii.
[27] *Id*. at 22.
[28] *Id*. at 22-23.
[29] Press Release, TRUSTe, Behavioral Advertising: Not that Bad?! TRUSTe Survey Shows Decline in Concern for Behavioral Advertising – Consumers Want Relevant Ads Online, But Still Worry About Their Online Privacy (Mar. 4, 2009) ("TRUSTe Survey"), *available at* http://www.truste.org/about/press_release/03_04_09.php.

that they do not consistently take the necessary steps to do so."[30] TRUSTe suggests that this supports arguments why identity theft remains a major privacy concern.[31] It also demonstrates that consumers may not fully understand how to take advantage of certain privacy protections offered by businesses. At the very least, the TRUSTe survey reveals that consumers are uncomfortable that the disclosure of financial or other sensitive information may result in an invasion of their privacy, identity theft, credit card theft, or the unauthorized sharing of health and financial records.[32]

The collection of online data related to children, moreover, raises numerous privacy concerns. Children have proven to be early adopters of Internet and wireless technologies and are often more proficient than their parents in using computers, mobile devices, MP3 players, and game consoles. Having been born into a digital society, children are more comfortable disclosing personal information, such as gender, age, location, and hobbies, as well as providing real-time status updates regarding their daily habits, on sites like MySpace, Facebook, and Bebo. Because children are both avid Internet users and consumers of entertainment, music, sports, and clothing, companies highly value the marketing profiles culled from their online activity.[33] Advocacy groups are concerned about advertisers targeting children.[34]

Behavioral advertising practices also raise privacy concerns with some users because they believe that data profiling can be used for harmful purposes. Companies can create

---

[30] *Id*.
[31] *Id*.
[32] *Id*. (listing that of the consumer respondents, 35% felt that their privacy was violated due to information they provided over the Internet; 6% reported having their identity stolen in 2008; 11% experienced credit card theft in the last year; and 13% reported unauthorized sharing of highly sensitive personal information over the last year).
[33] *See* CDD/PIRG Supplement at 42-44.
[34] First, children may not possess the requisite capacity to understand a company's privacy policy or procedures or consent to such practices. Second, privacy disclosures may fail to describe the type of content that will be delivered or how children's mobile numbers will be shared. Third, such advertisements could reach children below the intended target age, could be delivered to children 13 years old or younger without parental consent, and could prove manipulative as the targeted advertisements for certain brands are seamlessly integrated into the online domains of social networking sites. *See, e.g.*, FTC Mobile Marketing Report at 29; CDD/PIRG Supplement at 49-53.

consumer profiles by aggregating consumers' traffic across search engines or by mining log files of user activity across unrelated sites over time.[35] In assembling user profiles, companies can capture demographic data, such as gender, age, ethnicity, household income, marital status, home ownership, political status, sexual orientation, religious beliefs, and personal interests. The profiles are then organized by categories that advertisers can target ads against. Although companies represent that they use data only for relevant advertising, concerns persist and will only be dispelled by significant steps to provide more transparency about such data users.

Additional privacy concerns are on the horizon. In addition to increasing broadband access, President Obama has championed alternative energy production by building a smart grid to reduce inefficiencies in the delivery of power to consumers. Smart grids increase the connectivity, automation, and coordination of energy transmission and distribution between suppliers, networks, and consumers. Smart grid technology also could expand energy efficiency into the home by monitoring consumers' energy usage in real time and communicating with household devices that respond to demands to shut off during periods of non-use (*e.g.*, during the work day, when businesses require more power resources). However, the opportunities and benefits of developing the smart grid also come with potential privacy risks. While key elements of the smart grid have yet to be defined, the planned design contemplates the integration of an advanced broadband and data flow metering functionality. This design feature raises questions about who will have access to individual user data (*i.e.*, how much electricity an individual uses, which rooms they are in, when, and how often). Finally, it also raises privacy concerns regarding whether individual devices may be identified or tracked.

With the benefits of ubiquitous access to the Internet and increased service capability,

[35] TRUSTe Whitepaper at 7; CDD/PIRG Supplement at 68 (citing the 28th International Data Protection and Privacy Commissioners' Conference).

new business models will emerge that will enhance users' experience; however, such expanded models may seek to collect and use more personal data through the methods discussed above, or may foster new ways to collect and aggregate data. Thus, now is the time to address seriously the privacy issues, to build consumers' confidence that will lead to their continued and expanded use of broadband resources.

IV. To Safeguard Consumers and Promote Broadband Adoption and Use, the Commission Should Ensure that its National Broadband Plan Addresses the Critical Privacy Elements of Transparency and Control

As discussed above, ubiquitous access to the broadband Internet, along with advanced services and applications with increased data speeds, provides consumers with significant benefits and opportunities. However, consumers will only use these advanced tools and take advantage of the available content if they believe that such data collection activities are being done on their behalf and subject to their control. As noted, many consumers are unaware of the data practices that are occurring and, more importantly, are unaware of how their own personal data is being collected, shared, and used by companies. Thus, the issues of transparency and control are paramount.

A. Companies Should Recognize That They Have an Ongoing Relationship with Their Customers and Should Focus on Improving Transparency and Control.

Companies continue to offer new technologies and innovative broadband services and applications to consumers, which increasingly involve the collection or transfer or consumer data. Companies need to recognize that they have an ongoing relationship with their customers and that continued trust from their customers is critical to maintaining that relationship.[36] Therefore,

[36] *See* Network Advertising Initiative, *2008 NAI Principles – The Network Advertising Initiative's Self-Regulatory Code of Conduct*, 3 ("NAI Principles"), *available at* http://networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf ("Even where there is reduced privacy impact in use of anonymous or anonymized data, the NAI recognizes that consumers will

companies should ensure that if they are making decisions related to a consumer's personal information, the consumer also has a voice in the decision-making process. Specifically, as new services are deployed, Internet companies need to focus on providing improved transparency and control to consumers with respect to their data collection and use practices.

Transparency. Currently, company disclosures regarding the collection and use of an individual's personal information are generally made through online privacy policies. Often, these disclosures are inadequate. Many Web users do not understand these lengthy privacy policies, which use technical language such as "personally identifiable information," "Web beacons," and "behavioral targeting."[37] Moreover, the definitions of these and other important terms often differ. FTC Chairman Jon Leibowitz has stated "[m]ost current online privacy policies are essentially incomprehensible for even the savviest online users."[38]

Although privacy policies will continue to play an important role in legally binding companies to commitments and providing essential details regarding their data practices, widespread agreement now exists that more candid, prominent, and engaging methods are needed to ensure that trustworthy and meaningful communications are provided to users. As FTC Commissioner Harbour noted, "[d]isclosures about information collection, use, and control are not meaningful if they are buried deep within an opaque privacy policy that only a lawyer can understand."[39] Although users do not want to read lengthy privacy policies, companies nonetheless must inform consumers about their data collection and use practices before consumers can meaningfully consent to those practices.

---

only trust and continue to engage with advertisers online when there is appropriate deference shown to consumers' concerns about the privacy of their websurfing experience.").

[37] *See* Harbour Statement at 3, 10.

[38] Wendy Davis, *Can WPP Demystify Behavioral Targeting?*, THE DAILY ONLINE EXAMINER, May 20, 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=106519 (last accessed June 8, 2009).

[39] Harbour Statement at 4.

To increase transparency, Internet companies should provide consumers with complete, accurate information about their data collection and use practices. According to the FTC's recently released Staff Report on Self-Regulatory Principles for Online Behavioral Advertising (the "Principles"), Web sites should provide a "clear, concise, consumer-friendly, and prominent statement that data about consumer's activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests."[40] In addition, companies also should ensure that adequate steps are taken to protect consumer data against loss, unauthorized access, or other misuse. Moreover, because many consumers find existing disclosures difficult to understand, companies should work towards making the disclosures easier to read and understand. A recent TRUSTe survey indicates that as companies increase the level of transparency associated with their information collection and behavioral advertising practices, consumer comfort also increases.[41] Through these steps, businesses must not only provide more transparent privacy disclosures and increased comfort to consumers, but they also must educate consumers about the benefits of targeted advertising and a personalized online experience.

Control. To strengthen consumer trust further, companies also need to provide consumers with increased control over the data collection and use process. Consumers need adequate tools to allow them to make informed decisions over how their personal information should be used and shared (and the transparent disclosures and processes discussed above can assist with informed decision-making). Consumers also need appropriate mechanisms to exercise their informed decisions.

The Principles also highlight the importance of consumer control. Under the Principles,

[40] FTC Principles at 46.
[41] TRUSTe Survey.

Web sites should provide a "transparent" notice so consumers can choose whether to have their information collected for behavioral advertising purposes, along with a "clear, easy-to-use, and accessible method" for exercising that choice.[42] Moreover, when companies collect consumer data through sources other than a traditional Web site (*e.g.*, through mobile devices), the Principles state that such companies should provide customer choice mechanisms tailored to those communications.[43]

As businesses deploy enhanced privacy and data collection features that provide consumers with additional control over their personal information, they should educate consumers about these features. However, companies also need to provide certainty to consumers that their choices regarding data practices will be honored. If a consumer elects not to have their personal information collected or shared, companies need to respect that decision. As FTC Commissioner Harbour noted, "once consumers exercise their choices, companies must be held accountable for the promises they make to consumers regarding collection and use of personal data."[44]

Enhanced control facilitates data use that is obvious, useful, intuitive, and valuable to the consumer. By providing additional features and tools to support increased consumer control and online autonomy, broadband providers and online companies can ensure that consumers are served by their data and not enslaved by the ubiquity of the Internet.

B. FPF is Working to Advance Transparency and Consumer Control.

As noted above, FPF is working to promote transparency and control in data practices that will enhance consumer trust and enable privacy and personalization. FPF is committed to documenting current practices and developing reports detailing how consumer data is obtained

[42] FTC Principles at 46.
[43] *Id.*
[44] Harbour Statement at 1-2.

and used.[45]

FPF recently announced a major research initiative that will examine different methods for communicating with users about online advertising and privacy practices.[46] The study is exploring potential tools and notices that could be used by companies across the industry to raise consumer awareness about the use of behavioral advertising data. As part of the study, FPF is working with a team of creative experts and research specialists to develop a variety of consumer notices and test them with users. The research will include input from the general public and other creative experts about effective ways to inform consumers about behavioral advertising practices.

FTC Commissioner Harbour issued a statement in support of the FPF project and said, "[m]ost consumers do not fully understand the types and amount of information collected by businesses, or why the information may be commercially valuable. To the extent that the industry currently attempts to provide notice and choice to consumers, such efforts are insufficient. It is my hope that this research will help educate the industry and government about more effective ways to communicate with users and remove any confusion consumers may have about data use."[47] Many industry players that support the FPF initiative are beginning to look seriously at new innovative and more effective ways of communicating with their users about behavioral advertising. The project looks to build upon these efforts by specific companies and by industry groups to help find meaningful ways to engage users. FPF hopes to release materials from the initial phase of the research by the end of this summer.

---

[45] For example, FPF has developed a "Consumer Tool Kit" that includes a central opt-out list for consumers that want to opt-out of behavioral and targeted advertising. The Took Kit also includes information on the privacy tools available in Internet browsers, how to control Flash cookies, and links to additional online privacy resources. Future of Privacy Forum Consumer Tool Kit, http://www.futureofprivacy.org/2008/11/12/consumer-tool-kit/ (last accessed June 8, 2009).

[46] FPF Research Initiative.

[47] *Id*.

C. Internet Companies Should Help Provide Privacy Solutions.

Internet companies — including ISPs, online service companies and browser developers — should also help advance the transparency of and consumer control over online privacy practices. As noted above, the FTC has already signaled that these companies need to improve upon the existing privacy policy paradigm. Only then can consumers begin to understand fully how their own personal data is being collected, shared, and used.

To further transparency and consumer control, new approaches to consumer privacy should simplify the user experience. For example, companies could provide an intuitive user "dashboard" that indicates the types of data being collected and shared. The dashboard could also include various "controls" with which the user could select specific information (or categories of information) to share with various parties. Furthermore, the dashboard could be used to explain the benefits of data collection, including personalized content and other elements of a customized experience.

An additional barrier to the current model for consumer control online is the reliance on an opt-out cookie to manage user privacy choices. As FTC Commissioner Harbour stated, "[t]he primary mechanism by which consumers currently can exercise choice online — the opt-out cookie — is fundamentally flawed."[48] Opt-out cookies, used primarily to disable behavioral advertising, are routinely deleted by consumers, removed by anti-spyware programs, or overwritten and corrupted. User preferences are thus nullified against their wishes and without their knowledge. The Commission should consider examining the steps that can be taken by browser companies, Web sites, and ISPs to improve user controls in this area.

ISPs in particular should focus on how to ensure that their advertising related practices support user privacy. So-called DPI advertising and related practices by some providers have

[48] Harbour Statement at 4-5.

already raised concerns from privacy advocates, as these practices may "discourage consumers from 'access[ing] the lawful Internet content of their choice.'"[49] FPF is pleased that leading ISPs have committed to proceed with such advertising only with clear consumer consent, and it urges others to join in voluntarily making the same commitment.

Some companies are already experimenting with new privacy mechanisms. Google, for example, recently announced that it would begin to give users the ability to see and edit the information that it has compiled about their interests for the purposes of behavioral advertising. Yahoo! and eBay have experimented with efforts to provide enhanced notice to users by labeling banner ads with notices about behavioral advertising and links to opt-out choices. Other companies such as Lotame are beginning to provide users with browser plug-ins which help ensure that opt-out cookies stay in place to secure better the choices made by users.

V. A Mix of Government Oversight of Privacy and Data Security and Self-Regulation are Beginning to Drive Improved Industry Practices

A. Privacy and Data Security Issues Implicated by Widespread Broadband Use are Receiving Significant Attention From Federal, State, and International Government Bodies.

Ongoing government oversight of privacy and data security issues in the United States and abroad demonstrates that there is a growing consensus in support of ensuring that consumer privacy practices incorporate transparency and control.

1. FTC Report: Self-Regulatory Principles for Online Behavioral Advertising (February 2009).

Since 1995, the FTC has explored and evaluated "data collection practices, industry self-regulatory efforts, and technological developments affecting consumer privacy" in the online

[49] *NOI* ¶ 59, citing *Internet Policy Statement*, 20 FCC Rcd 14986, 14988 ¶ 4 (2005).

marketplace.[50] This year, FTC Staff released the Principles to encourage more robust industry self-regulation to protect consumer privacy better in the context of online behavioral advertising. The Principles are designed to address legitimate privacy concerns without destroying the benefits of online behavioral advertising. Because previous self-regulatory models proved too "cumbersome" with "inaccessible opt-out system[s]," failed to provide consumers with meaningful control over the tracking of their online activities, and were limited in their application and enforcement, the Principles specifically include the four governing concepts of (i) transparency and consumer control, (ii) reasonable security and limited data retention for consumer data, (iii) express consumer consent to material retroactive changes to privacy promises, and (iv) express consumer consent to the use of sensitive data for behavioral advertising.[51] Although the Principles are not formal rules and do not alter companies' obligations to comply with federal and state laws and privacy policies, they reflect widespread support for conspicuous consumer notice and choice and include transparency and consumer control as top priorities for best practices.[52]

2. FTC Mobile Marketing Report (April 2009).

In April 2009, shortly after Staff released the Principles, the FTC published a staff report surveying the mobile marketplace (the "Report"), which details discussions from nine public town hall sessions on topics ranging from current trends in the mobile marketplace to location-based services to the privacy concerns that arise with increased mobile advertising.[53] According to the Report, the mobile advertising industry likely will flourish as it capitalizes on new marketing opportunities where banner ads, text messaging campaigns, and targeted

[50] FTC Principles at i.
[51] *Id*. at 9-10, 46-47.
[52] *See id*. at 46. FTC Chairman Jon Leibowitz has emphasized that industry members have significant work to do in order to achieve more meaningful self-regulation that satisfies the Principles' goals. *Id*. at iv, 48.
[53] FTC Mobile Marketing Report.

advertisements based on location information derived directly from the consumers' mobile device can be delivered to the consumers' mobile phones.[54] The Report noted that industry members widely agree that privacy practices in the mobile marketplace should incorporate two key tenets of consumer privacy—notice and consent.[55] Although the FTC stated that it applauds industry participation in addressing consumer privacy issues, the FTC plans to continue to police the wireless space to ensure consumer protection.[56]

3. Congress.

Congress, too, has taken notice of individuals' increased use of the Internet for social and business activities and the resultant incentive for companies to track such online behavior for advertising purposes. Concerns about the lack of transparency regarding the scope of these information gathering practices has prompted both the House and the Senate to investigate the privacy implications of online advertising and DPI. Such hearings and soon-to-be-introduced legislation illustrate the congressional commitment to protecting consumer privacy through enhanced disclosures and consumer control over online consumer tracking.

In the past year, Congress has held multiple hearings with industry participants, such as AT&T Services, Google, Microsoft, NebuAd, the Center for Democracy and Technology, Spark Capital, and BroadbandPolitics.com, covering (1) monitoring consumer usage on broadband and wireless networks through DPI and Global Positioning System tracking,[57] (2) balancing

---

[54] *Id*. at 7, 16, and 20.

[55] *Id*. at 22. Town hall panelists indicate that different levels of notice and consent are appropriate depending on the mobile advertising activity (*e.g.*, banner ads warrant a notice and opt-out option; disclosure of a user's location as part of a family and friend finder application warrants a notice and opt-in option; recurring notices are appropriate when sharing location-based information with certain services; and text messaging ad campaigns should require the consumer to opt-in twice). *Id*. at 19-20, 22.

[56] *Id*. at 43.

[57] *Communications Networks and Consumer Privacy: Recent Developments: Hearing Before the H. Subcomm. on Comm., Technology & the Internet*, 111th Cong. (Apr. 23, 2009), *available at* http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1590:energy-and-commerce-subcommittee-hearing-on-communications-networks-and-consumer-privacy-recent-developments&catid=134:subcommittee-on-communications-technology-and-the-internet&Itemid=74.

broadband providers' use of DPI with protecting consumers' privacy,[58] and (3) the privacy implications of online advertising.[59] In a Senate Commerce, Science and Transportation Committee hearing, Senator Inouye and former-Senator Stevens remarked that industry must ensure that consumers' personal information is safeguarded online and that their online activity should not be tracked without their knowledge or notice.[60] In another hearing, the House Subcommittee on Telecommunications and the Internet expressed support for broadband providers' use of DPI to manage network congestion and protect against viruses, but found that using such technology to track customers' Internet use without providing notice or a mechanism to opt in or out to be "deeply troubling."[61] In the current session of Congress, legislation focused on enhanced consumer privacy will soon be introduced.[62]

4. States.

Several states have passed data security and privacy laws to safeguard consumers' personal information and to improve transparency and control. Generally, these laws require businesses that own, license, collect, process, or use personal information to implement reasonable measures to protect that information. For example, California, Connecticut, Rhode

---

[58] *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies: Hearing Before the H. Subcomm. On Telecomm. & the Internet*, 110th Cong. (2008) ("DPI House Hearing"), *available at* http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1264&catid=18:platforms&Itemid=58.

[59] *Privacy Implications of Online Advertising: Hearing Before the S. Comm. On Commerce, Sci. & Transp.*, 110th Cong. (2008), *available at* http://commerce.senate.gov/public/index.cfm?FuseAction+Hearings.Hearing&Hearing_ID=e46b0d9f-562e-41a6-b460-a714bf37017.

[60] *Id.*, Statement of Senator Inouye, *available at* http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Statement&Statement_ID=45a83c01-b624-4173-adae-b54cc1a79cc9; *id.*, Statement of Senator Stevens, *available at* http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Statement&Statement_ID=ed1128f1-0a95-4b4a-80c6-9689cb32ca86.

[61] DPI House Hearing.

[62] Angela Moscaritolo, *Behavioral Advertising Bill Being Drafted*, SC MAGAZINE, Mar. 16, 2009, *available at* http://www.scmagazineus.com/Behavioral-advertising-bill-being-drafted/article/128882/ (reporting that three Congressmen reportedly drafted legislation — the details of which remain unknown — requiring companies to inform consumers that their online activity is being tracked for advertising purposes).

Island, and Texas require businesses to adopt appropriately tailored and reasonable practices to prevent the personal information of their residents from being unlawfully disclosed, destroyed, modified, or accessed.[63] Massachusetts and Nevada laws have gone even further by mandating comprehensive security plans or encryption for protecting residents' personal information.[64]

The California Online Privacy Protection Act requires Web sites' privacy policies to explain what information is collected, how that information is shared and used, how a consumer can review and rectify personal information if allowed by the operator, how a consumer can learn of changes to the privacy policy, and the currency of the policy itself.[65] Nevada and Minnesota, moreover, require ISPs to prevent the disclosure of customer's PII, and Minnesota additionally requires ISPs to get customer consent before disclosing information about subscribers' online activities.[66] Finally, the New York State Assembly has considered the proposed "New York Online Consumer Protection Act," which, if passed, would prohibit Web sites and advertising networks from collecting consumers' PII for the purposes of behavioral

[63] *See, e.g.*, CAL. CIV. CODE §§ 1798.80-1798.84 (governing businesses use of customer's personal data); CONN. GEN. STAT. § 42-471 (safeguarding personal information and establishing disposal requirements for such data); R.I. GEN. LAWS § 11-49.2-2 (requiring businesses that own or license personal information about residents to provide reasonable security for that information); TEX. BUS. & COM. CODE § 521.052 (establishing that businesses have a duty to protect customers' sensitive personal information).

[64] 201 MASS. CODE. REGS. 17.00 (mandating that entities that maintain personal information develop a security plan that meets specific requirements, four of which include (i) contractually obligating third-party service providers that access personal information to safeguard the data, (ii) minimizing the length of time personal information is stored, (iii) documenting all actions taken in response to a security breach, and (iv) creating an inventory of all computer systems, storage media, and paper and electronic records to indentify those that contain personal information); NEV. REV. STAT. § 597.970 (requiring businesses within the state to encrypt customer's personal information before electronically transmitting it a person outside the secure system).

[65] CAL. BUS. & PROF. CODE §§ 22575-22579. Although there is no national privacy law that requires Web sites to provide consumer notice regarding data collection practices, the California Online Privacy Protection Act has become the *de facto* national standard to the extent that Web sites collect personal information from California residents. California also requires all nonfinancial businesses to disclose to customers in writing the type of the information the businesses share or sell to third parties for marketing purposes or compensation. *See* CAL. CIV. CODE §§ 1798.83-1798.84.

[66] NEV. REV. STAT. § 205.498; MINN. STAT. §§ 325M.01-.325M.09.

advertising without consent.[67]

5. International.

a. European Union.

In 1995, the European Commission implemented Directive 95/46/EC,[68] known as the Data Protection Directive ("EU Directive"), which regulates the processing of individuals' personal data within the European Union ("EU").[69] The principles governing the EU Directive are transparency, legitimate purpose, and consumer choice. The EU Directive expressly requires that the data collector inform the user of this practice and explain the purpose behind such processing.[70] Because the EU does not favor indiscriminate processing of personal data, Article 7 of the EU Directive preserves consumer choice and limits when such data may be used—it requires the user's unambiguous consent to such actions, except in certain narrow circumstances.[71] Moreover, the user has the right to access, without excessive delay or expense, all data processed relating to his or her identity, learn the purpose for the processing and for whom it is being collected, and amend or delete the collected data.[72] The user also has the right to object to, among other things, the processing of personal data for direct marketing or the disclosure of such information to third parties for direct marketing.[73] Because American companies operating within the EU must comply with the EU Directive and operate using global

---

[67] Assemb. B. A01393, 2009 Leg., Reg. Sess. (N.Y. 2009), *available at* http://assembly.state.ny.us/leg/?bn=A01393. The bill also requires that Web sites give consumers adequate notice of how advertisers collect and use data, as well as a clear and conspicuous mechanism to opt-out of such online advertising.

[68] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("EU Directive"), *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm .

[69] The EU Directive was designed to harmonize the disparate privacy and data protection laws of the Member States, so all Member States were required to update their national legislation per the EU Directive by October 1998.

[70] EU Directive at Art. 10 (requiring the data controller or its representative to inform the user of the identity of the controller, the purpose for the processing, the recipients of the data, whether disclosure of such information by the user is obligatory or voluntary and the consequences for failing to reply, and the right to access and correct collected personal data); *see also id.* at Art. 11.

[71] EU Directive at Art. 7.

[72] *Id*. at Art. 12.

[73] *Id*. at Art. 14.

platforms, many also afford U.S. consumers the same level of transparency and choice when collecting personal data stateside. For example, when Google, Yahoo!, and Microsoft adopted data retention limits for their search data in order to comply with the opinions of EU data regulators, they adopted these practices for U.S. consumers as well.

b. Canada.

Building consumers' trust and confidence in commercial activities, especially those carried out in the online marketplace, also is a key tenet of Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA").[74] Specifically, PIPEDA establishes ten principles, which are based on the Canadian Standards Association Model Code for the Protection of Personal Information, that private sector organizations must follow when collecting, using, and disclosing consumers' personal information in the course of commercial activities.[75] These principles include indentifying the purpose(s) of the data collection, requiring consumer consent in certain circumstances, mandating openness about the organization's policies and practices regarding use of the personal information, and providing the consumer with notice that his or her information is being used and that he or she may access and correct it.[76]

The federal, state, and international legislative framework that currently exists and that is under consideration reflects a keen awareness of the importance of online privacy.

B. Industry Members are Continuing to Develop Leading Practices for Nascent Broadband Technologies, Consistent with the FTC's Guidance and Other Incentives.

In addition to the continuing examination of privacy issues by governmental entities,

---

[74] *See* PIPEDA, *available at* http://laws.justice.gc.ca/en/P-8.6/index.html; *see also* Industry Canada, *The Digital Economy in Canada – Privacy for Business*, *at* http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00464.html.
[75] *Id.*; Office of the Privacy Commissioner of Canada, *A Guide for Businesses and Organizations Your Privacy Responsibilities*, at http://www.priv.gc.ca/information/guide_e.cfm. Additionally, Canada's Privacy Act (R.S., 1985, C. P-21) governs the government's collection, use, and disclosure of individual's personal information. *See* http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-21///en.
[76] *See* PIPEDA at Schedule 1, *available at* http://laws.justice.gc.ca/en/showdoc/cs/P-8.6/sc:1//en#anchorsc:1.

industry participants in the broadband sphere are actively developing a series of best practices designed to promote transparency and control and protect consumer privacy and data security. These organizations, including FPF, are committed to advancing privacy practices to improve the consumer experience. Over time, these organizations have developed a significant amount of research on consumer privacy expectations—particularly with respect to the use of broadband services and technologies. The Commission therefore should take these industry initiatives into account as it develops a national broadband plan.

1. The Network Advertising Initiative.

The Network Advertising Initiative ("NAI") is a cooperative of online marketing and analytics companies committed to advancing responsible privacy and data security practices. Formed in 1999 in response to concerns related to behavioral advertising, the NAI works with policymakers and the online industry to promote "strong and balanced privacy protections" that focus on consumer notice, choice, control, and dispute resolution. In 2000, the NAI adopted the NAI Principles, a set of self-regulatory guidelines for online advertising. Last year, NAI released an updated set of Principles to account for new technologies and evolving business models in online advertising.[77]

Transparency and consumer choice are the leading NAI Principles.[78] NAI requires its members to maintain the NAI Web site as a "centralized portal offering explanations of online behavioral advertising and member companies' compliance with the NAI Principles."[79] In addition, members are required to use reasonable efforts to "educate consumers about behavioral advertising, and the choices available to consumers with respect to behavioral advertising"

[77] *See* NAI Principles. The NAI has also developed standards for 3rd party ad networks and cookies, spam, and Web beacons, *available at* http://www.networkadvertising.org/about/.
[78] NAI Principles at 7-8.
[79] *Id.* at 7.

(including through the NAI Web site).[80] The principles also emphasize that the level of consumer choice is tied to the sensitivity of the underlying data and how the data will be used by the NAI member.[81] Importantly, the Principles provide that the use of "sensitive consumer information" (which currently includes social security numbers, insurance plan and financial account numbers, real-time geographic location information, and certain medical information, among other information) requires opt-in consent from users.[82]

2. TRUSTe.

Another organization working to advance online privacy practices is TRUSTe, whose reports are cited above.[83] Founded in 1997, TRUSTe helps preserve online privacy and promote transparency and consumer control through its Privacy and Safe Harbor Seals, Trusted Download programs, and other initiatives. As of 2008, more than 3,400 Web sites participated in TRUSTe's Seal programs.[84]

To assist parents and ensure child safety, TRUSTe has developed a specialized Children's Privacy Seal.[85] TRUSTe has been approved by the FTC as a Safe Harbor provider under the Children's Online Privacy Protection Act, and the Children's Seal certifies that a Web site is COPPA-compliant and is "child-friendly." Participants in the Children's Seal program also must abide by TRUSTe's standard Privacy Seal requirements, including ongoing site monitoring and the Watchdog Dispute Resolution program. TRUSTe also released an online

[80] *Id.*
[81] *Id.* at 8.
[82] *Id.* at 6, 8.
[83] TRUSTe Web site, http://www.truste.org (last accessed June 8, 2009).
[84] TRUSTe currently offers a Privacy Seal, Email Privacy Seal, Children's Privacy Seal, EU Safe Harbor Seal, and Japan Privacy Seal.
[85] TRUSTe, Brand Your Web site as 'Child-friendly' with TRUSTe, http://www.truste.org/businesses/childrens_privacy_seal.php (last accessed June 8, 2009).

privacy tutorial specifically targeted at parents and teachers.[86]

TRUSTe has also been committed to advancing privacy in the behavioral advertising context. Earlier this year, TRUSTe issued a whitepaper entitled "Online Behavioral Advertising: A Checklist of Practices that Impact Consumer Trust" (the "Whitepaper").[87] The Whitepaper discusses evolving behavioral advertising models and privacy practices and highlights the need for transparency and choice in obtaining trust from online consumers. In addition, the Whitepaper includes a checklist for businesses to use as they review their data collection and privacy practices for compliance with law and best practices.

3. Interactive Advertising Bureau.

Founded in 1996, the Interactive Advertising Bureau ("IAB") is comprised of more than 375 leading media and technology companies focused on the growth of interactive marketing.[88] Collectively, these members are responsible for selling 86% of online advertising in the United States.[89] Through numerous councils, committees, and working groups, IAB has become a leader in developing standards and best practices.

As part of its commitment to protecting online consumer privacy, the IAB has been coordinating a joint effort with the Direct Marketing Association, the Association of National Advertisers, the American Advertising Association, and the Online Publishers Association to seek to reach agreement on a set of enhanced behavioral advertising principles. The principles, which are still under negotiation, are intended to comply with the FTC's demand for an enhanced self regulatory regime in the area of behavioral advertising.

---

[86] TRUSTe, *Online Privacy: A Tutorial for Parents and Teachers, available at* http://www.truste.org/pdf/parent_teacher_tutorial.pdf.
[87] TRUSTe Whitepaper.
[88] About the IAB, http://www.iab.net/about_the_iab (last accessed June 8, 2009).
[89] *Id.*

4. The Mobile Marketing Association.

The Mobile Marketing Association ("MMA") has also been very active in identifying and developing best practices for behavioral advertising and other marketing activities via mobile devices. MMA has more than 700 members, including "agencies, advertisers, hand held device manufacturers, carriers and operators, retailers, software providers and service providers," along with other companies involving in mobile marketing.[90] With a "primary focus" on consumer protection and privacy, MMA's efforts focus on six "fundamental elements": choice, control, customization, consideration, constraint, and confidentiality.[91]

As part of its efforts to protect mobile users from unwanted communications, MMA has developed a "Global Code of Conduct" for marketers that make use of consumer data to market their products and services to those users via mobile devices.[92] The key principles of transparency and control permeate the Code. For example, under the Code, mobile marketers must provide users with an easily understandable and quickly discoverable description of the terms and conditions of a marketing program. Moreover, marketers must obtain opt-in consent from users for all mobile messaging programs and limit the number of messages to those that have been requested. In addition, marketers must ensure that user information collected for marketing purposes should be used to tailor marketing to the user. Finally, the code requires marketers to implement "reasonable technical, administrative, and physical procedures" to protect user information against unauthorized use or access.[93]

---

[90] About the MMA, http://www.mmaglobal.com/about (last accessed June 8, 2009); FAQs, http://www.mmaglobal.com/about/faqs (last accessed June 8, 2009).
[91] Consumer, http://www.mmaglobal.com/consumer (last accessed June 8, 2009).
[92] Code of Conduct, http://www.mmaglobal.com/policies/code-of-conduct (last accessed June 8, 2009).
[93] MMA has also released a set of Consumer Best Practices Guidelines for mobile marketers, and these Guidelines incorporate provisions designed to improve transparency and consumer control. The Guidelines recognize that wireless subscribers have a right to privacy and that content providers must obtain approval from subscribers before sending messages and content. In addition, the guidelines provide detailed guidance covering a broad range of marketing issues, including opt-in and opt-out procedures, subscription practices, and customer care. The guidelines

5. CTIA – The Wireless Association.

Like MMA, CTIA – The Wireless Association has developed Best Practices Guidelines to protect mobile users.[94] Targeted at providers of "location-based services" ("LBS"), the guidelines apply "regardless of the technology or mobile device used or the business model employed to provide services."[95] The guidelines also stress the importance of user notice and consent in ensuring adequate consumer privacy.[96] In addition, the guidelines include provisions designed to ensure that LBS providers take reasonable measure to ensure protect the security and integrity of location information, and that they retain the information only as long as business needs require.[97]

---

also include a dedicated section on marketing to children. *See* Consumer Best Practices Guideline, http://www.mmaglobal.com/policies/consumer-best-practices (last accessed June 8, 2009).

[94] CTIA Best Practices and Guidelines for Location Based Services, *available at* http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.

[95] *Id.* at 1.

[96] *Id.*

[97] *Id.* at 6-7.

VI. Conclusion

For the foregoing reasons, the Commission should emphasize the importance of privacy issues in the national broadband plan, and it should take into account the progress and the potential gaps in the ongoing legal, legislative, regulatory, and self-regulatory activity advance online privacy.

Respectfully submitted,

/s/ Christopher Wolf

Christopher Wolf
Co-Chairman
Jules Polonetsky
Co-Chair and Director
THE FUTURE OF PRIVACY FORUM
919 18th Street, NW
Washington, DC 20036
www.futureofprivacy.org

Christopher Wolf
Mark W. Brennan
Sarah P. Reisert
HOGAN AND HARTSON
555 13th Street, NW
Washington, DC 20004
(202) 637-8834
Facsimile: (202) 637-5910
E-mail: cwolf@hhlaw.com
Counsel for THE FUTURE OF PRIVACY FORUM

June 8, 2009