

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Comments Sought on Privacy Issues) GN Docket Nos. 09-47, 09-51, 09-137
Raised by the Center for Democracy and)
Technology)
)
NBP Public Notice #29)
)

VERIZON COMMENTS – NBP PUBLIC NOTICE #29

At Verizon,¹ protecting the privacy of customer information is an important and longstanding priority. Verizon remains committed to maintaining strong and meaningful privacy protections for consumers in this era of rapidly changing technological advances, including those involving broadband. The many innovations in information use and technology that have enriched the consumer experience have been the direct result of the existing system of self-governance, with collaboration and engagement by parties throughout all parts of the Internet ecosystem and minimal governmental involvement. There is nothing to suggest a different approach is needed with respect to consumer privacy on the Internet today. Nonetheless, if government involvement in this area somehow becomes necessary, the Commission should avoid any duplication of the Federal Trade Commission’s (FTC) ongoing efforts, including its Privacy Roundtable Series² that examines many of the issues raised in Public Notice #29.³ Given the FTC’s

¹ In addition to Verizon Wireless, the Verizon companies participating in this filing (“Verizon”) are the regulated, wholly owned subsidiaries of Verizon Communications Inc.

² FTC, Exploring Privacy: A Roundtable Series, <http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml> (last visited Jan. 22, 2010) (“Privacy Roundtable Series”).

broader jurisdiction over entities in the broadband ecosystem, such as application providers and Web site publishers, the Commission must also be careful to avoid any inconsistency to ensure that all providers are treated evenly.

DISCUSSION

As Verizon and Google explained in their recent joint filing,⁴ players in the Internet ecosystem should, in the first instance, set the norms of behavior and operation, including those relating to consumer privacy. The Internet community is highly motivated and well positioned to police itself, especially if all players are committed to transparency and inclusiveness. Going forward, it remains critical to preserve this system of self-governance, with governmental involvement limited to dealing with bad actors on a case-by-case basis where industry mechanisms are unable to resolve conduct that is anticompetitive and harms consumers.

Should government involvement in Internet consumer privacy issues become necessary, the FTC has an important role in light of the questions surrounding the Commission's jurisdiction that have been raised.⁵ By contrast, it is settled that the FTC has jurisdiction over many of the entities that collect consumer information in the broadband ecosystem – e.g., Web site publishers and providers of applications, browsers,

³ *Comments Sought on Privacy Issues Raised by the Center for Democracy and Technology*, Public Notice, GN Docket Nos. 09-47, 09-51 & 09-137; DA 10-62 (Jan. 13, 2010) (“Public Notice #29”).

⁴ See Google and Verizon Joint Submission on the Open Internet, *Preserving the Open Internet*, GN Docket No. 09-191, at 3 (Jan. 14, 2010).

⁵ See, e.g., *id.* at 3 (suggesting that “government agencies of general jurisdiction, such as the U.S. Federal Trade Commission” address consumer issues rather than “communications regulatory bodies, such as the FCC” that “are agencies of limited jurisdiction”); Comments of Electronic Frontier Foundation, *Preserving the Open Internet*, GN Docket No. 09-191, at 6-10 (Jan. 14, 2010) (“Congress has not deputized the FCC to be a free roving regulator of the Internet.”).

toolbars, search engines, and downloadable software. Because Public Notice #29 addresses consumer privacy issues that are implicated when *any* entity uses consumer information collected via the Internet, there should be a single approach to consumer privacy in the broadband space, and the Commission should avoid any inconsistency with the FTC to ensure a level playing field for all entities that participate there.

The Commission should also avoid duplication since the FTC has considerable experience dealing with consumer privacy issues related to the Internet. Most recently, in late 2009, the FTC launched an ongoing Privacy Roundtable Series to explore consumer privacy issues raised by recent developments in technology and business practices. Verizon submitted comments in response to questions the FTC posed in each of the first two roundtables. (Verizon's comments are attached as Exs. 1 and 2.) Within these comments, Verizon addressed many of the topics raised in Public Notice #29. While the Privacy Roundtables were not limited to broadband privacy issues, Verizon's comments covered all of its services, including fixed and wireless broadband. And the same privacy concerns raised in Public Notice #29 are already being considered by the FTC outside the broadband context as well.

In particular, Verizon made the following points in its FTC comments that are pertinent to Public Notice #29:

Consumer Expectations of Privacy. Verizon's longstanding commitment to transparency, customer choice, and consumer education drives its actions with regard to privacy, and the highly competitive nature of our industry reinforces this commitment.. For example, Verizon's understanding of its customers' opposition to a national wireless directory led Verizon to vigorously oppose those plans. While Verizon's efforts to

respond to consumer privacy expectations have been recognized by consumers and privacy experts alike,⁶ Verizon remains acutely aware that consumer expectations evolve rapidly as new technologies and services become available and consistently strives to meet those expectations.

Building Privacy by Design. Verizon considers privacy issues and the appropriate data protection measures as it plans for and develops products and services for its customers. Verizon strives to build privacy controls into new products and services at the outset in order to make such controls as effective and comprehensive as possible. To protect sensitive customer data, Verizon employs various technical security measures, such as de-identification, encryption, and data aggregation. The use of such measures should be commensurate with the sensitivity of the specific information being protected, the amount of time the data is present, and the purpose(s) for which the data is used. Moreover, data should be retained only for as long as is necessary to fulfill both legitimate business needs and any obligations to retain specific information.⁷ Companies – not government agencies – are in the best position to understand the type of data they collect, and to decide the best manner and level of protection for securing that data and the length of time to keep that data. Companies also require ample flexibility to engage in practices, such as network management, to protect themselves and the data they collect from attacks as the recent cyber attacks attributed to China vividly demonstrate.

⁶ Ponemon Institute and TRUSTe Rank America's Most Trusted Companies in Privacy, http://www.truste.com/about_TRUSTe/press-room/news_truste_2009_most_trusted_companies_for_privacy.html (Sept. 16, 2009) (last visited Jan. 22, 2010).

⁷ For example, the Commission's Part 42 rules require that carriers retain telephone toll records for 18 months and all other records for the period established in the carrier's data retention index. See 47 CFR §§ 42.6-.7. Moreover, companies may be required to retain data for law enforcement purposes.

Privacy Obligations of Platform Providers and Third-Party Application

Providers. As the proliferation of Internet innovations and experience in the wireless industry shows, consumers enthusiastically welcome third-party applications and make purchasing decisions based on the availability of such applications.⁸ At the same time, these third-party applications raise new challenges for consumers seeking safeguards and control over the information about them that is generated, collected, and used by these applications.

As is currently the case, platform providers, government agencies, consumer groups, and others may assist consumers by providing them with educational resources, such as guidance regarding Internet safety and the avoidance of scams, and may also be able to assist customers if their privacy is violated by unscrupulous actors. However, under no circumstances should a platform provider be liable for the actions of third-party application providers. The platform provider cannot reasonably be expected to know of or monitor all third-party applications that a consumer may download on his or her PC or wireless device.⁹ Nor can a provider force independent third-party application providers to adhere to a specific set of information collection, use, or security measures. Even if providers were able to screen all applications for their platforms, such a vetting process

⁸ See, e.g., *IDC Predictions 2010: Recovery and Transformation*, IDC #220987, Vol. 1, <http://cdn.idc.com/research/predictions10/downloads/Top10Predictions.pdf> (Dec. 2009) (“[2010] will be a watershed year in the ascension of mobile devices as strategic platforms for commercial and enterprise developers as over 1 billion access the Internet, iPhone apps triple, Android apps quintuple, and Apple’s ‘iPad’ arrives.”).

⁹ See, e.g., “Mobile Apps Business is Booming...for Apple,” PCWorld, http://www.pcworld.com/businesscenter/article/187200/mobile_apps_business_is_booming_for_apple.html (Jan. 19, 2010) (last visited Jan. 22, 2010) (“Apple has over 150,000 apps available, and... estimates project that it will have more than 300,000 apps by the end of 2010.... The Android Market has already built an impressive library of apps – with more than 20,000 apps and rising.”).

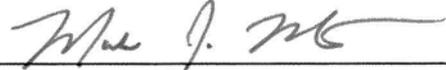
would considerably delay consumers' use of valued applications and likely deter application providers from developing new applications. Screening applications based on certain privacy criteria would also be inconsistent with the principle that platform providers should allow full access to all lawful applications on their platforms.

In a world of increasingly diverse third-party service offerings, consumers must take responsibility for investigating the privacy policies of the application providers with which they are sharing their information and selecting those that meet their expectations with regard to information collection and use practices. Application providers should adhere to the principle of meaningful disclosure so that consumers will have the opportunity to understand the privacy implications that come with the use of a particular application or service. And application providers should bear the responsibility to secure and appropriately use the consumer data they collect. As a result of consumers making informed choices, the marketplace would reward those application providers that provide valuable services to the customer with the desired level of privacy protection.

CONCLUSION

Self-governance, collaboration with parties throughout the Internet ecosystem, and minimal governmental involvement have allowed the explosive innovation in services and applications that has developed to respond to consumers' evolving needs and enrich the consumer experience. To the extent government intervention in Internet consumer privacy issues becomes necessary, the Commission should avoid inconsistency with and duplication of the FTC's efforts.

Respectfully submitted,



Karen Zacharia
Mark J. Montano
VERIZON
1320 North Courthouse Road
9th Floor
Arlington, VA 22201
(703) 351-3158

Attorneys for Verizon

Michael E. Glover
Of Counsel

January 22, 2010

EXHIBIT 1

**VERIZON COMMENTS IN CONNECTION WITH
THE FEDERAL TRADE COMMISSION’S ROUNDTABLE SERIES:
EXPLORING PRIVACY
[Privacy Roundtables – Comment, Project No. P095416]**

Verizon¹ recognizes the Federal Trade Commission’s longstanding commitment to consumer privacy, and shares its goal of determining how best to protect consumer privacy while supporting beneficial uses of information and technological innovation. We appreciate the opportunity to provide comments in connection with this important series of roundtable discussions.

At Verizon, protecting the privacy of customer information is an important and longstanding priority. We remain committed to maintaining strong and meaningful privacy protections for consumers in this era of rapidly changing technological advances. We know that consumers will use the full capabilities of our communications products, services and networks only if they trust that their information will remain private. Trust that a company has strong privacy practices and respects consumers’ privacy preferences is important to many consumers as they select an organization with which to do business. We were gratified when independent privacy experts recently ranked Verizon the most trusted communications company for privacy, reinforcing our longstanding commitment to giving our customers the high standard of privacy protection they deserve.²

As discussed below, we believe that while there may be challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data, innovations in information use and technology have enriched the consumer experience and will continue to do so as long as they recognize consumer privacy concerns and are coupled with robust privacy protections.

**I. RISKS, CONCERNS, AND BENEFITS ARISING FROM THE
COLLECTION, SHARING, AND USE OF CONSUMER INFORMATION**

**A. Retail or other commercial environments involving a direct
consumer-business relationship.**

The collection, sharing, and use of consumer information in the direct retail consumer-business relationship is critically important to Verizon’s ability to provide high-quality

¹ In addition to Verizon Wireless, the Verizon companies participating in this filing (“Verizon”) are the regulated, wholly owned subsidiaries of Verizon Communications Inc. While preserving its rights under the common carrier exemption of the FTC Act, Verizon welcomes the FTC’s initiative with regard to these privacy roundtables.

² Ponemon Institute and TRUSTe Rank America’s Most Trusted Companies in Privacy, Sept. 16, 2009, available at: http://www.truste.com/about_TRUSTe/press-room/news_truste_2009_most_trusted_companies_for_privacy.html.

products and services to our customers, to develop and offer new products and services, and to create a positive experience for our customers and Web visitors. We collect and use information about our customers and Web site visitors for a variety of purposes. Information may be obtained when customers order and use our products and services, when they make customer service inquiries, or when consumers visit our Web sites. We use this information to deliver, provide, and repair products or services; establish and maintain customer accounts and billing records; better direct specific offers or promotions to customers and Web site visitors; monitor Web site statistics; monitor our customer service employees; or authenticate customers' online accounts. By doing so, we facilitate their ability to receive efficient, responsive, and timely service on a 24/7 basis, and ensure our ability to provide the desired products and services.

We recognize that consumers may have concerns about the use of their information for marketing purposes. Therefore, we provide customers with a range of choices about how we share and use information for such purposes. Verizon does not sell, license, or share information that individually identifies customers with third parties for their own marketing purposes. If customer information is shared with third-party vendors or agents who do specific work on Verizon's behalf, our contracts prohibit them from using the information for any other purposes. Our privacy practices for certain services also are subject to Federal Communications Commission ("FCC") regulations, including regulations regarding Customer Proprietary Network Information ("CPNI"). Consistent with existing CPNI regulations, customers may instruct us not to use their CPNI for marketing categories of services different from those they currently have. In addition, consumers may opt out of receiving marketing solicitations from Verizon via calls, emails, postal mailings, text messages, or door-to-door contact.

The collection, sharing, and use of customer information come with a concomitant obligation to protect the security of that information. At Verizon, we have technical, administrative and physical safeguards in place to help protect against unauthorized access to, use or disclosure of customer information we maintain. Employees are trained on the importance of protecting privacy and on the proper access to, use and disclosure of customer information. Under our security practices and policies, access to personally identifiable information is authorized only for those who have a business need for such access, and records are to be retained only as long as necessary for business or legal needs. Sensitive personally identifiable records are to be destroyed before disposal. Recognizing that no program can be 100 percent secure, Verizon has incident response plans in place to handle incidents involving unauthorized access to personal information. Verizon also has a strong commitment to Internet safety, and provides educational resources and tools to help customers protect themselves from phishing, spam, pretexting, viruses, and other scams that they may encounter and that might threaten their private information.

B. The mobile environment.

As mentioned above, we provide our customers with choices about the sharing and use of their information, including in the mobile environment. Advances in wireless

technology, especially the growing availability of location-based services, hold great potential for consumer benefit – including convenience and safety – but also bring new concerns about how customer information is used and shared. As a member of CTIA, Verizon Wireless follows the industry Best Practices and Guidelines for Location-Based Services,³ whose hallmarks are user notice and consent. Toward that end, we provide our wireless customers with clear notice regarding how these types of services work and require that they make the choice about whether specific location-tracking features available on their phones are turned on when using their wireless phones. Customers are given the opportunity to choose where and when to turn specific location-based services on and off.

In addition, Verizon Wireless does not support or participate in the development of a national wireless phone number directory. We do not publish directories of our customers' wireless phone numbers, and we do not provide or make them available to third parties for listing in directories unless customers request that we do so.

C. Behavioral advertising.

The use of consumers' Web-surfing data to foster targeted online advertising raises important issues regarding online privacy. Consumers deserve clear and transparent notice of the types of targeted advertising practices that service providers and Web sites employ. If certain practices cause consumers to be concerned that their privacy will not be protected, or that their preferences won't be respected, they will be less likely to trust their online services, thereby diminishing the consumer benefits provided by the Internet.

Verizon believes that any technology that is used to track and collect consumer online behavior across non-affiliated Web sites for the purposes of behavioral advertising – regardless of the company doing the collecting – should only be used with the customer's knowledge and consent in accordance with appropriate self-regulatory safeguards and best practices. We believe that transparent customer notice requires conspicuous, clearly explained disclosure to consumers about the types of data collected and the purpose for which that data is being used. With that disclosure, consumers should be able to exercise meaningful choice and control, on an ongoing basis, as to whether their information may be collected and used for online behavioral advertising. In addition, we believe that any company engaged in tracking and collecting such information must have appropriate security controls in place to guard against unauthorized access to any personal information.

Consistent with these beliefs, Verizon participated in the development of the cross-industry Self-Regulatory Principles for Online Behavioral Advertising⁴ announced this summer by leading advertising industry associations. The Principles represent a

³ CTIA Best Practices and Guidelines for Location-Based Services, April 2, 2008, available at http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf.

⁴ Self-Regulatory Principles for Online Behavioral Advertising, July 2009, available at <http://www.iab.net/media/file/ven-principles-07-01-09.pdf>.

comprehensive effort to establish and commit to consumer-friendly practices for online advertising across the entire advertising industry, including Web publishers, advertisers, advertising networks, and companies that provide services such as Internet access, tool bars, Web browsers and other comparable desktop applications and client software.

The Principles serve as the online advertising industry's initial response to the FTC's call to action regarding online behavioral advertising, which urged industry to raise the bar and do better with respect to transparency and consumer choice. Once implemented, the Principles will provide consumers with greater transparency, choice and control regarding the use of their Web-surfing activities for online behavioral advertising purposes. The Principles also include an important commitment to consumer education, giving consumers a consistent understanding of online behavioral advertising practices regardless of the company or Web site with which they are interacting. We believe that widespread and uniform adoption of these Principles will greatly enhance the public trust, address privacy concerns, and serve as a foundation for further discussion with policymakers and consumer groups.

Verizon also recognizes that policymakers and consumer groups have expressed concerns regarding new technologies that might be employed to gather information about customers' Web-surfing activities across unrelated Web sites for the purpose of interest-based advertising. Verizon does not gather information from our customers' use of our broadband access services to determine their Web-surfing activities across non-Verizon sites for the purpose of providing them with interest-based advertisements. If Verizon engages in this type of online behavioral advertising, we will provide customers with clear and meaningful notice of our practice and obtain their affirmative consent.

D. Sensitive information.

Verizon's corporate policies require heightened protection of sensitive data. As mentioned above, we often are in possession of sensitive information, such as Social Security numbers and financial account numbers, to provide and bill for our products and services. As a major employer, we also maintain an array of employee data. We maintain strong controls for the protection of such data.

We also believe that heightened protections should be required with regard to the collection or use of sensitive data for purposes such as online advertising. We join the FTC and others in recognizing, however, that the term "sensitive data" needs to be more precisely and carefully defined. While sensitive personal information such as Social Security numbers or financial account numbers should not be collected for purposes of behavioral advertising, a one-size-fits-all prohibition on the use of broad categories of information could have unintended consequences, including undermining Internet users' experience.

In addition, special attention should be given to protecting information of a sensitive nature (e.g., accessing medical Web sites). This information should not be collected and used for online behavioral advertising unless specific affirmative consent and customer

controls are in place to limit such use. Specific policies may be necessary to deal with this type of information.

Consistent with our longstanding policies and practices, Verizon also believes that the content of communications, such as email, instant messages, or VoIP calls, should not be used, analyzed, or disclosed for purposes of Internet-based targeted advertising.

II. CONSUMER EXPECTATIONS ABOUT HOW INFORMATION CONCERNING CONSUMERS IS COLLECTED AND USED

Our understanding of consumer expectations about the collection and use of their information help drive Verizon's actions with regard to privacy. For example, understanding our customers' preferences led Verizon Wireless to vigorously oppose plans to create a national wireless directory. We also know that consumers often look for certain signs that allow them to feel confident about their privacy when they use our Web sites. To meet those expectations, Verizon Web sites contain a link to our comprehensive privacy policy, display the TRUSTe and Better Business Bureau ("BBB") Online seals, and use the "lock icon" and the "https" prefix to assure customers that their credit card and other sensitive information is transmitted securely. Likewise, as we developed our recently revised comprehensive privacy policy, we listened to consumer feedback we obtained through surveys and meetings. The feedback regarding consumer readability and ease-of use, for example, were instrumental in our decisions regarding both the structure and content of the policy.

While our efforts to respond to consumer privacy expectations have been recognized by consumers and privacy experts alike, we remain acutely aware that consumer expectations evolve rapidly as new technologies and services become available. For example, privacy expectations and concerns may be changing with the introduction of social media services and new wireless applications, and may vary across generations. As discussed above, Verizon believes that our continuing strong commitment to transparency, customer choice and consumer education will ensure that we remain in the forefront of privacy protection.⁵

III. EXISTING LEGAL REQUIREMENTS AND SELF-REGULATORY REGIMES IN THE UNITED STATES TODAY

Verizon believes that current legal authority, coupled with robust enforcement where appropriate, will continue to be effective in protecting consumer privacy interests, and

⁵ The highly competitive nature of our industry and our direct-to-consumer relationship reinforce this commitment. Competition spurs good privacy practices where consumers have a direct relationship with the privacy-protecting entity and understand what it is doing to protect them from privacy threats. Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. ____ (2010) (forthcoming).

urges careful consideration before proceeding with additional laws or regulations. An extensive body of state and federal law – ranging, for example, from state data-breach notification statutes to the federal Children’s Online Privacy Protection Act to the FCC’s CPNI regulations to the FTC’s Section 5 authority – provides a solid framework for safeguarding consumer privacy. This existing framework has proven capable and effective in addressing challenges arising from innovations in information use and technology.

Where additional protections are necessary, self-regulatory regimes act as a powerful and effective complement to governmental action, as demonstrated by the BBB Advertising Review Services,⁶ the CTIA Best Practices and Guidelines for Location-Based Services, and the recently released Self-Regulatory Principles for Online Behavioral Advertising. Members of a particular industry are uniquely positioned to understand the way in which their business works, and how best to effect the sector-wide response necessary to protect consumer privacy while allowing market and technical innovations to continue. Self-regulation also can offer greater flexibility in responding effectively and promptly to new concerns, helping industry stay a step ahead of emerging threats.

IV. CONCLUSION

Verizon supports the FTC’s continuing examination of how best to protect consumer privacy while supporting beneficial uses of information and technological innovation. We look forward to participating in this important dialogue.

⁶ BBB Advertising Review Services, available at <http://www.bbb.org/us/Advertising-Review-Services/>.

EXHIBIT 2

**VERIZON COMMENTS IN CONNECTION WITH
THE FEDERAL TRADE COMMISSION’S ROUNDTABLE SERIES:
EXPLORING PRIVACY
[Privacy Roundtables – Comment, Project No. P095416]**

Verizon¹ recognizes the Federal Trade Commission’s longstanding commitment to consumer privacy, and shares its goal of determining how best to protect consumer privacy while supporting beneficial uses of information and technological innovation. We appreciate the opportunity to provide comments in connection with this important series of roundtable discussions.

At Verizon, protecting the privacy of customer information is an important and longstanding priority. We remain committed to maintaining strong and meaningful privacy protections for consumers in this era of rapidly changing technological advances. We know that consumers will use the full capabilities of our communications products, services and networks only if they trust that their information will remain private. Trust that a company has strong privacy practices and respects consumers’ privacy preferences is important to many consumers as they select an organization with which to do business. We were gratified when independent privacy experts recently ranked Verizon the most trusted communications company for privacy, reinforcing our longstanding commitment to giving our customers the high standard of privacy protection they deserve.²

As discussed below, we believe that while there may be challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data, innovations in information use and technology have enriched the consumer experience and will continue to do so as long as they recognize consumer privacy concerns and are coupled with robust privacy protections.

**I. RISKS, CONCERNS, AND BENEFITS ARISING FROM THE
COLLECTION, SHARING, AND USE OF CONSUMER INFORMATION**

**A. Retail or other commercial environments involving a direct
consumer-business relationship.**

The collection, sharing, and use of consumer information in the direct retail consumer-business relationship is critically important to Verizon’s ability to provide high-quality

¹ In addition to Verizon Wireless, the Verizon companies participating in this filing (“Verizon”) are the regulated, wholly owned subsidiaries of Verizon Communications Inc. While preserving its rights under the common carrier exemption of the FTC Act, Verizon welcomes the FTC’s initiative with regard to these privacy roundtables.

² Ponemon Institute and TRUSTe Rank America’s Most Trusted Companies in Privacy, Sept. 16, 2009, available at: http://www.truste.com/about_TRUSTe/press-room/news_truste_2009_most_trusted_companies_for_privacy.html.

products and services to our customers, to develop and offer new products and services, and to create a positive experience for our customers and Web visitors. We collect and use information about our customers and Web site visitors for a variety of purposes. Information may be obtained when customers order and use our products and services, when they make customer service inquiries, or when consumers visit our Web sites. We use this information to deliver, provide, and repair products or services; establish and maintain customer accounts and billing records; better direct specific offers or promotions to customers and Web site visitors; monitor Web site statistics; monitor our customer service employees; or authenticate customers' online accounts. By doing so, we facilitate their ability to receive efficient, responsive, and timely service on a 24/7 basis, and ensure our ability to provide the desired products and services.

We recognize that consumers may have concerns about the use of their information for marketing purposes. Therefore, we provide customers with a range of choices about how we share and use information for such purposes. Verizon does not sell, license, or share information that individually identifies customers with third parties for their own marketing purposes. If customer information is shared with third-party vendors or agents who do specific work on Verizon's behalf, our contracts prohibit them from using the information for any other purposes. Our privacy practices for certain services also are subject to Federal Communications Commission ("FCC") regulations, including regulations regarding Customer Proprietary Network Information ("CPNI"). Consistent with existing CPNI regulations, customers may instruct us not to use their CPNI for marketing categories of services different from those they currently have. In addition, consumers may opt out of receiving marketing solicitations from Verizon via calls, emails, postal mailings, text messages, or door-to-door contact.

The collection, sharing, and use of customer information come with a concomitant obligation to protect the security of that information. At Verizon, we have technical, administrative and physical safeguards in place to help protect against unauthorized access to, use or disclosure of customer information we maintain. Employees are trained on the importance of protecting privacy and on the proper access to, use and disclosure of customer information. Under our security practices and policies, access to personally identifiable information is authorized only for those who have a business need for such access, and records are to be retained only as long as necessary for business or legal needs. Sensitive personally identifiable records are to be destroyed before disposal. Recognizing that no program can be 100 percent secure, Verizon has incident response plans in place to handle incidents involving unauthorized access to personal information. Verizon also has a strong commitment to Internet safety, and provides educational resources and tools to help customers protect themselves from phishing, spam, pretexting, viruses, and other scams that they may encounter and that might threaten their private information.

B. The mobile environment.

As mentioned above, we provide our customers with choices about the sharing and use of their information, including in the mobile environment. Advances in wireless

technology, especially the growing availability of location-based services, hold great potential for consumer benefit – including convenience and safety – but also bring new concerns about how customer information is used and shared. As a member of CTIA, Verizon Wireless follows the industry Best Practices and Guidelines for Location-Based Services,³ whose hallmarks are user notice and consent. Toward that end, we provide our wireless customers with clear notice regarding how these types of services work and require that they make the choice about whether specific location-tracking features available on their phones are turned on when using their wireless phones. Customers are given the opportunity to choose where and when to turn specific location-based services on and off.

In addition, Verizon Wireless does not support or participate in the development of a national wireless phone number directory. We do not publish directories of our customers' wireless phone numbers, and we do not provide or make them available to third parties for listing in directories unless customers request that we do so.

C. Behavioral advertising.

The use of consumers' Web-surfing data to foster targeted online advertising raises important issues regarding online privacy. Consumers deserve clear and transparent notice of the types of targeted advertising practices that service providers and Web sites employ. If certain practices cause consumers to be concerned that their privacy will not be protected, or that their preferences won't be respected, they will be less likely to trust their online services, thereby diminishing the consumer benefits provided by the Internet.

Verizon believes that any technology that is used to track and collect consumer online behavior across non-affiliated Web sites for the purposes of behavioral advertising – regardless of the company doing the collecting – should only be used with the customer's knowledge and consent in accordance with appropriate self-regulatory safeguards and best practices. We believe that transparent customer notice requires conspicuous, clearly explained disclosure to consumers about the types of data collected and the purpose for which that data is being used. With that disclosure, consumers should be able to exercise meaningful choice and control, on an ongoing basis, as to whether their information may be collected and used for online behavioral advertising. In addition, we believe that any company engaged in tracking and collecting such information must have appropriate security controls in place to guard against unauthorized access to any personal information.

Consistent with these beliefs, Verizon participated in the development of the cross-industry Self-Regulatory Principles for Online Behavioral Advertising⁴ announced this summer by leading advertising industry associations. The Principles represent a

³ CTIA Best Practices and Guidelines for Location-Based Services, April 2, 2008, available at http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf.

⁴ Self-Regulatory Principles for Online Behavioral Advertising, July 2009, available at <http://www.iab.net/media/file/ven-principles-07-01-09.pdf>.

comprehensive effort to establish and commit to consumer-friendly practices for online advertising across the entire advertising industry, including Web publishers, advertisers, advertising networks, and companies that provide services such as Internet access, tool bars, Web browsers and other comparable desktop applications and client software.

The Principles serve as the online advertising industry's initial response to the FTC's call to action regarding online behavioral advertising, which urged industry to raise the bar and do better with respect to transparency and consumer choice. Once implemented, the Principles will provide consumers with greater transparency, choice and control regarding the use of their Web-surfing activities for online behavioral advertising purposes. The Principles also include an important commitment to consumer education, giving consumers a consistent understanding of online behavioral advertising practices regardless of the company or Web site with which they are interacting. We believe that widespread and uniform adoption of these Principles will greatly enhance the public trust, address privacy concerns, and serve as a foundation for further discussion with policymakers and consumer groups.

Verizon also recognizes that policymakers and consumer groups have expressed concerns regarding new technologies that might be employed to gather information about customers' Web-surfing activities across unrelated Web sites for the purpose of interest-based advertising. Verizon does not gather information from our customers' use of our broadband access services to determine their Web-surfing activities across non-Verizon sites for the purpose of providing them with interest-based advertisements. If Verizon engages in this type of online behavioral advertising, we will provide customers with clear and meaningful notice of our practice and obtain their affirmative consent.

D. Sensitive information.

Verizon's corporate policies require heightened protection of sensitive data. As mentioned above, we often are in possession of sensitive information, such as Social Security numbers and financial account numbers, to provide and bill for our products and services. As a major employer, we also maintain an array of employee data. We maintain strong controls for the protection of such data.

We also believe that heightened protections should be required with regard to the collection or use of sensitive data for purposes such as online advertising. We join the FTC and others in recognizing, however, that the term "sensitive data" needs to be more precisely and carefully defined. While sensitive personal information such as Social Security numbers or financial account numbers should not be collected for purposes of behavioral advertising, a one-size-fits-all prohibition on the use of broad categories of information could have unintended consequences, including undermining Internet users' experience.

In addition, special attention should be given to protecting information of a sensitive nature (e.g., accessing medical Web sites). This information should not be collected and used for online behavioral advertising unless specific affirmative consent and customer

controls are in place to limit such use. Specific policies may be necessary to deal with this type of information.

Consistent with our longstanding policies and practices, Verizon also believes that the content of communications, such as email, instant messages, or VoIP calls, should not be used, analyzed, or disclosed for purposes of Internet-based targeted advertising.

II. CONSUMER EXPECTATIONS ABOUT HOW INFORMATION CONCERNING CONSUMERS IS COLLECTED AND USED

Our understanding of consumer expectations about the collection and use of their information help drive Verizon's actions with regard to privacy. For example, understanding our customers' preferences led Verizon Wireless to vigorously oppose plans to create a national wireless directory. We also know that consumers often look for certain signs that allow them to feel confident about their privacy when they use our Web sites. To meet those expectations, Verizon Web sites contain a link to our comprehensive privacy policy, display the TRUSTe and Better Business Bureau ("BBB") Online seals, and use the "lock icon" and the "https" prefix to assure customers that their credit card and other sensitive information is transmitted securely. Likewise, as we developed our recently revised comprehensive privacy policy, we listened to consumer feedback we obtained through surveys and meetings. The feedback regarding consumer readability and ease-of use, for example, were instrumental in our decisions regarding both the structure and content of the policy.

While our efforts to respond to consumer privacy expectations have been recognized by consumers and privacy experts alike, we remain acutely aware that consumer expectations evolve rapidly as new technologies and services become available. For example, privacy expectations and concerns may be changing with the introduction of social media services and new wireless applications, and may vary across generations. As discussed above, Verizon believes that our continuing strong commitment to transparency, customer choice and consumer education will ensure that we remain in the forefront of privacy protection.⁵

III. EXISTING LEGAL REQUIREMENTS AND SELF-REGULATORY REGIMES IN THE UNITED STATES TODAY

Verizon believes that current legal authority, coupled with robust enforcement where appropriate, will continue to be effective in protecting consumer privacy interests, and

⁵ The highly competitive nature of our industry and our direct-to-consumer relationship reinforce this commitment. Competition spurs good privacy practices where consumers have a direct relationship with the privacy-protecting entity and understand what it is doing to protect them from privacy threats. Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. ____ (2010) (forthcoming).

urges careful consideration before proceeding with additional laws or regulations. An extensive body of state and federal law – ranging, for example, from state data-breach notification statutes to the federal Children’s Online Privacy Protection Act to the FCC’s CPNI regulations to the FTC’s Section 5 authority – provides a solid framework for safeguarding consumer privacy. This existing framework has proven capable and effective in addressing challenges arising from innovations in information use and technology.

Where additional protections are necessary, self-regulatory regimes act as a powerful and effective complement to governmental action, as demonstrated by the BBB Advertising Review Services,⁶ the CTIA Best Practices and Guidelines for Location-Based Services, and the recently released Self-Regulatory Principles for Online Behavioral Advertising. Members of a particular industry are uniquely positioned to understand the way in which their business works, and how best to effect the sector-wide response necessary to protect consumer privacy while allowing market and technical innovations to continue. Self-regulation also can offer greater flexibility in responding effectively and promptly to new concerns, helping industry stay a step ahead of emerging threats.

IV. CONCLUSION

Verizon supports the FTC’s continuing examination of how best to protect consumer privacy while supporting beneficial uses of information and technological innovation. We look forward to participating in this important dialogue.

⁶ BBB Advertising Review Services, available at <http://www.bbb.org/us/Advertising-Review-Services/>.