Before the
FEDERAL TRADE COMMISSION

Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"	)))))	File No. P095456

COMMENTS OF VERIZON AND VERIZON WIRELESS

Kathleen G. Zanowic
Chief Privacy Officer
VERIZON
1320 North Court House Road, 9th Floor
Arlington, Virginia 22201
(703) 351-3156

Karen Zacharia
Magnolia Mansourkia
Jamellah Ellis
Christopher Oatway
VERIZON
1320 North Court House Road, 9th Floor
Arlington, Virginia 22201
(703) 351-3199

John T. Scott, III
VERIZON WIRELESS
1300 I Street N.W., Suite 400 West
Washington, DC 20005

February 18, 2011

TABLE OF CONTENTS

Before the
FEDERAL TRADE COMMISSION

Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"	)))))	File No. P095456

COMMENTS OF VERIZON AND VERIZON WIRELESS ON THE PRELIMINARY FTC STAFF REPORT ENTITLED "PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS"

Verizon[1] supports the Federal Trade Commission (FTC) Staff's efforts to craft a framework that guides the commercial use of consumer information while safeguarding consumer privacy and simultaneously fostering continued economic growth and innovation. The Staff's framework[2] appropriately contemplates that these goals may be accomplished through the expansion and ongoing implementation of industry best practices and self-regulatory programs.

Verizon agrees with the FTC that there must be a balance "to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits offered by the ever-changing marketplace."[3] Three key principles should guide the FTC as it finalizes its framework aimed at achieving this balance. *First*, the framework should focus on the protection of consumer data and its use, and not on

[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] The framework is contained in the preliminary FTC Staff report entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (Dec. 2010) ("Preliminary Staff Report").

[3] Prepared Statement of the Federal Trade Commission on Do Not Track, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, U. S. House of Representatives, http://www.ftc.gov/os/testimony/101202donottrack.pdf, at 2 (Dec. 2, 2010).

the technology used to collect data, or the business model underlying data collection and use, or the corporate structure or affiliation of the entity collecting and using the data. The framework must apply broadly and evenly. *Second*, in view of the rapid technological advancements and the ever-growing multitude of products, services, and industry players, a framework that is too prescriptive or that forces one-size-fits-all requirements will halt innovation and disserve consumers. The framework must be flexible. *Third*, privacy protections should be proportionate to the sensitivity of the data being collected and the intended uses of that data. Against these principles, Staff's carefully crafted framework – emphasizing privacy by design, simplified consumer choice, and increased transparency in data practices – can provide guidance to industry-developed self-regulatory programs and corporate best practices for consumer privacy protection.

With respect to Staff's recommendations regarding privacy by design, Verizon agrees that consumer privacy protections should inform the product and service development process and should be reflected in corporate data security, collection, and retention practices. At the same time, however, rigid or prescriptive requirements in these areas would be counterproductive and should be avoided. For example, companies should be provided with the necessary flexibility to implement reasonable retention periods based on record types and other business-specific needs and uses.

Verizon also shares Staff's view that decisions regarding the appropriateness of consumer notice and consent models should be driven by the sensitivity of the consumer data involved and its use. By scaling notice and consent relative to data type *and* use, companies can improve the utility and relevancy of privacy decision-making within the

user experience, and supply meaningful notice and choice options. Again, a set of specific regulations is not indicated here; instead, Verizon urges the FTC to support and encourage ongoing development and implementation of industry self-regulatory efforts, and to look to these programs for best practices regarding notice and choice that the FTC may want to endorse. For example, concerning choice in the online behavioral advertising context, Staff proposes a Do Not Track mechanism that would enable consumers to opt-out of participating in certain behavioral advertising programs, but industry's adoption of the Self-Regulatory Principles for Online Behavioral Advertising – including the implementation of a common icon – addresses the activity that is the focus of Staff's proposed Do Not Track mechanism. This comprehensive program should be given a chance to work before alternatives are considered. Similarly, while Staff correctly notes that there are "commonly accepted practices" for which consumer consent to data usage is unnecessary, attempts to enumerate these practices may prove impractical. A definition of commonly accepted practices that is too narrow could effectively exclude common data uses such as certain affiliate marketing programs, common uses of aggregated data, and first-party marketing practices. A static list also would not account for the evolving nature of data use practices that may become commonplace in the future in response to consumer demand.

Finally, with respect to transparency, Verizon supports Staff's goal of increasing the transparency of commercial data use practices to better ensure that consumers can make informed choices. Indeed, transparency principles inform existing industry best practices in areas such as privacy policies, advertising notices, and use of location data. These best practices should also inform the FTC as it finalizes its framework. Similarly,

consistent with Staff's recommendations, a consumer's ability to access data held by a company should be governed by a sliding scale where access is proportionate to the sensitivity of the data and its use. But any recommendation regarding consumer access to data must be balanced against the significant costs and technical challenges associated with providing large-scale access to data. As Staff recognizes, a reasonable middle ground may be to ensure that consumers have access to their *elections* about data usage, rather than access to the data itself.

DISCUSSION

I. Scope and Application of Proposed Framework.

A. The Scope of the Privacy Framework Must Be Carefully Defined, Must Apply Equally to All Entities, and Must Be Technologically Neutral.

The Preliminary Staff Report correctly calls for a privacy framework that applies broadly throughout both the online and offline economies.[4] The proposed framework applies to commercial entities that collect data that can be "reasonably linked to a specific consumer, computer or other device."[5] If this broad definition of scope is used, it is important that companies not be required to apply the same level of privacy controls to all types of data. Treating all data that can be reasonably linked to a device the same as data that actually identifies an individual, for example, is likely to create significant operational and implementation obstacles including service delivery issues (e.g., delivering Web content based on IP address information). Moreover, requiring the same data protection standards for any data element that might be

[4] Preliminary Staff Report at 42.

[5] *Id.*

reasonably linked to a device actually creates disincentives for keeping such data in a de-identified form.

Consumers expect and deserve a privacy framework that ensures consistent levels of privacy protections regardless of the entities with which they choose to interact or the technologies or techniques those entities employ to collect data. For example, if consent is required for the use of data for a particular purpose, the appropriate method for obtaining the consent may depend on a number of factors, including the entity's business practices or the way it collects the data (e.g., a call center, Web site, or retail store), but the *level* of consent should not vary.[6]

Yet, the Preliminary Staff Report distinguishes and unfairly focuses on Internet Service Providers (ISPs) and one specific technology – deep packet inspection – as necessitating completely different standards.[7] This heavy-handed view unfairly disadvantages ISPs and favors companies, technologies, and business models based on cookies and other technologies and software that collect and use similar (and perhaps a greater amount of) information. The underlying principles of meaningful notice and choice should apply across the board based on the type of information collected and how the information will be used, including whether and for what purpose it will be shared

[6] Under an evenly applied privacy framework, the particular technology used to gather data is not relevant. For example, Verizon recognizes the concerns consumers have expressed with regard to the collection of information from use of Verizon's broadband access services to determine Web browsing activities across non-Verizon sites for the purposes of providing interest-based advertisements. As such, Verizon's privacy policy states that if Verizon engages in this type of online behavioral advertising, customers will be provided with clear and meaningful notice of Verizon's practice and affirmative consent will be obtained. The technology Verizon could use to obtain such data is not relevant to this commitment. Similar collection of data and use for this purpose, regardless of the technology used to collect the data or the entity collecting it, should follow this affirmative meaningful consent standard.

[7] *See* Preliminary Staff Report at 62 (noting that deep packet inspection "would likely warrant enhanced consent or even more heightened restrictions").

with third parties. Consumers are not focused on technologies, business models, or service categories; they are focused on the privacy protections afforded their data, as well as transparency and choice.

In sum, failure to consistently apply the framework to all entities and practices would result in inconsistent data protection and competitive disadvantages. Inconsistent data protections may leave consumers confused and unable to understand what levels of protection and control are afforded them when dealing with different types of entities.

B. A Framework Focused on Promoting Industry Codes of Conduct Is Uniquely Suited to Address Diverse and Evolving Privacy Practices.

As the Department of Commerce observed in its recent privacy Green Paper, the diversity of services, business models, and organizations to which a privacy framework must apply would "counsel against attempting to develop comprehensive, prescriptive rules."[8] The framework should not promote prescriptive regulation that adversely affects consumer welfare by halting innovation and delaying the expansion of new and better products and services.[9] Therefore, to address this concern, Verizon supports the use of voluntary industry codes of conduct which are uniquely suited to buttress existing privacy laws and regulation. Unlike top-down government regulation, voluntary industry codes

---

[8] *See* U.S. Department of Commerce, Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf, at 32 (Dec. 2010).

[9] For example, one study concluded that delays in the introduction of voice messaging services due to line-of-business restrictions and delays in the introduction of cellular telephone service each imposed multi-billion dollar losses in consumer welfare. *See* Jerry Hausman et al., "Valuing the Effect of Regulation on New Services in Telecommunications," *Brookings Papers on Economic Activity, Microeconomics* Vol. 1997, at 1-54 (Martha V. Gottron and Anne Lesser, eds. 1997).

can efficiently and effectively apply baseline privacy principles to a variety of contexts, while also anticipating technological developments and evolving business practices.

Such a flexible framework is crucial in the privacy area because failures commonly result when regulators impose prescriptive rules based on isolated understandings or predictions about diverse and evolving technologies and industries. Prescriptive rules can quickly become obsolete – and worse, often lead to unintended negative consequences and may ultimately stifle investment and innovation. Policymakers "are often wrong both in their predictions of how the market will develop and in their judgments of what regulatory measures will best promote consumer welfare."[10]

II. Companies Should Promote Consumer Privacy Throughout Their Operations, and at Every Stage of the Development of their Products and Services.

.

A. Verizon is Committed to "Privacy by Design" and to Comprehensive Data Management Procedures.

Verizon agrees that companies should "promote consumer privacy throughout their organizations and at every stage of the development of their products and services."[11] Companies' privacy programs should also, as the Preliminary Staff Report indicates, include security measures appropriate for the sensitivity of the data.[12] Verizon employs robust privacy protection practices because its reputation for trust is an important business imperative and competitive asset.[13] Privacy is an integral part of

---

[10] Jonathan E. Neuchterlein and Philip J. Weiser, *Digital Crossroads: American Telecommunications Policy in the Internet Age*, at 428 (2005).

[11] Preliminary Staff Report at 44.

[12] *Id.* at 45.

[13] Verizon is proud to have received accolades for its strong commitment to privacy. For example, a comprehensive independent analysis of company privacy practices ranked Verizon as

Verizon's culture and is engrained in its business practices and policy positions. The concept of "privacy by design" is not new to Verizon. Privacy considerations have been incorporated into Verizon's product planning, development and implementation processes for decades. Data collection and use are essential considerations in these processes, as are data protection and security measures. For example, Verizon Wireless location-based services such as VZ Navigator or Family Locator[14] have built-in controls which require consumers to decide where and when to turn on the location-tracking features on their devices.[15]

B. Companies Should Have Flexibility to Adopt Reasonable Data Retention Practices.

The Preliminary Staff Report notes that "companies should implement reasonable and appropriate data retention periods."[16] Verizon agrees that reasonable retention periods are important, but the privacy framework must avoid prescriptive rules with specific data retention requirements. Retention periods often vary depending on business need, the type of data, the location of the data, the technical and operational issues

---

the most trusted communications company for its privacy practices. *See* "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). That study included a consumer survey as well as expert evaluations of Verizon's practices based on clarity and readability of privacy statements, access to account information, cookie management, and in- and out-of-network data-sharing practices.

[14] VZ Navigator is a mobile device application that allows subscribers to get turn-by-turn directions to a destination, search local places of interest, and obtain a searchable map of a particular location. Family Locator, formerly known as Chaperone, helps subscribers securely determine and receive updates on the location of family members' cell phones through a website or cell phone.

[15] In addition, customers may choose from a variety of parental control tools to protect children's privacy by blocking unwanted calls and messages, creating trusted numbers, or avoiding objectionable content.

[16] Preliminary Staff Report at 46.

associated with retaining the data in certain systems, and myriad legal requirements (including statutory law, law enforcement requirements, and potential discovery obligations in the context of civil litigation) to retain various types of documents that contain the data.

Data retention programs generally are based on record type, and not the data element in the record. Attempts to prescribe data deletion rules based on specific types of data (for example, a requirement that companies delete account information two years after a consumer has ended her relationship with a company) would likely create operational problems and conflict with legal obligations specific to particular industry segments. Companies need to maintain the ability to implement reasonable retention periods based on record type, multiple business needs, uses of particular data sets, and legal and regulatory requirements.

III. Companies Should Simplify Consumer Choice.

As Staff correctly notes, consumer notice and choice should be considered in proportion to the form and sensitivity of the data collected as well as its intended use. As noted in the Preliminary Staff Report, customers generally expect that a company they elect to do business with will use information about them for the purpose of delivering services and operating its business.[17] General customer notice, such as through a readily available privacy policy, about what data is collected and the purposes for which it will be used is appropriate for these operational and transactional uses. Consumers are also appropriately informed about data used for a company's research and development, performance measurement, analytics functions, first-party marketing, and certain

[17] *See* Preliminary Staff Report at 54.

advertising purposes through a general consumer notice. Soliciting consent for these practices is not only unnecessary but may diminish the impact of notice and choice that is offered for more sensitive practices. In contrast, consumers should be provided choice with respect to certain other types of data use. The actual choice mechanism offered to consumers and the means by which consumers inform the company of their data use preferences will appropriately vary with the data type, sensitivity, and use. As discussed further below, a flexible framework will facilitate appropriate consideration of sensitivity and use factors.

A. The Framework Should Account for the Evolving Nature of Commonly Accepted Practices.

Verizon agrees with Staff that there are "commonly accepted practices" for which companies should not be required to seek consent once the consumer elects to use a company's product or service. In many instances, consent is inferred because data use is obvious from the context of the transaction, or consent is simply not necessary because the use is sufficiently accepted or necessary for public policy reasons.[18] Staff views product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing as the "limited set" of data use practices that should be considered commonly accepted.[19] Verizon agrees that these data uses are appropriately categorized as "commonly accepted" and necessary such that a general notice to consumers about their uses is sufficient. Indeed, providing consumer choice in many of these instances would hamper companies in their ability to deliver a product or service.

[18] Preliminary Staff Report at 54-55.

[19] *Id*. at 53-55.

However, as explained below, Staff's limited set of commonly accepted practices excludes other practices that should be commonly accepted and defines some included practices too narrowly. And as technology evolves, existing or new practices may become so common that specific choice models adopted today may not make sense later. Therefore, rather than create an all-inclusive, narrowly-defined list of commonly accepted practices, the FTC should instead provide guidance on what might be considered commonly accepted.

For example, Staff notes that sharing consumer information with "service providers" acting at a company's direction for the purposes of product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing (provided there is no further use of the data) is considered commonly accepted.[20] However, the same scope and type of information-sharing among commonly branded affiliates should likewise be considered commonly accepted – yet that practice is excluded from Staff's limited set of commonly accepted practices. Similarly, the use of aggregate data – which is quite common and does not identify an individual – should not require a company to obtain individual consent. For example, aggregated data about customer product purchases within different market segments is often used to predict buying behaviors in similar markets and is also used to develop new product or package offerings. Aggregate data usually consists of demographic and statistical information (e.g., 100 males between ages 18 and 35) and cannot be used to identify an individual person or record. Thus, general notice about this type of data usage is appropriate. Indeed, existing law and industry guidelines except these types of

[20] *Id*. at 54-55.

aggregate data uses from the general prohibitions against using customer data for purposes outside of business operations.[21]

Furthermore, if practices that are deemed commonly accepted by the FTC are too narrowly defined, they may exclude data uses that consumers enjoy and have come to expect. For example, while Staff notes that first-party marketing is a commonly accepted practice for which companies should not be required to seek consent, Staff's proposed definition of first-party marketing – to include "only the collection of data from a consumer with whom the company interacts directly for purposes of marketing to that consumer"[22] – is too narrow. Companies routinely improve the relevancy of their product marketing advertisements to consumers by using demographic data obtained from third-party sources. Consumers typically expect and appreciate the benefits of this type of marketing and advertising.[23] Similarly, while Staff recognizes that first-party marketing allows for an online retailer to recommend products and services to consumers based on their prior purchases on the retailer's Web site,[24] the same retailer should have the ability to use offline channels to recommend products and services for which the

[21] *See*, for example, the provisions in the Communications Act addressing consumer proprietary network information, at 47 U.S.C. § 222 (c)(1) and (3). *See also* CTIA, "Best Practices and Guidelines for Location-Based Services," http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf, at Section 3 (April 2, 2008) ("CTIA Guidelines") (noting that the Guidelines do not apply to location information used or disclosed in the form of aggregate or anonymous data).

[22] Preliminary Staff Report at 55.

[23] Recent Verizon Wireless measurement data suggests that consumers click on ads that are behaviorally targeted seven times more often than they click on non-behaviorally targeted ads. Verizon Wireline advertising measurement data suggests that behaviorally targeted advertising results in a sale almost twice (1.8) as often as non-behaviorally targeted advertising.

[24] Preliminary Staff Report at 54.

consumers' prior online purchases suggest an interest.[25] Accordingly, an FTC framework that addresses commonly accepted practices must be sufficiently flexible to accommodate evolving data practices and uses that are reasonably expected by consumers.

B. Companies Must Consider the User Experience When Determining the Timing and Method of Presenting Notice and Choice.

Verizon agrees with Staff that consumers should be provided meaningful and accessible choice mechanisms and that, where feasible, choices should be offered at the point when the consumer is making a decision about providing data or deciding whether to use an application.[26] But the point at which notice and choice should be offered will necessarily differ depending on the context of the user experience. It is feasible for an online retailer to post a privacy policy in a location where a consumer can access it prior to making a purchase, but it would be impractical to require a call center representative to read a privacy policy to every incoming caller who is prepared to subscribe to a service. As long as consumers are given comprehensive notice and choice mechanisms in a timely manner and commensurate with the data type and intended use, companies should be able to reasonably implement the timing and method of presenting notice and choice.

To illustrate, mobile applications that use location data can be downloaded from a wireless carrier's application store as well as from a third-party application provider. Under the current CTIA Guidelines, if a user is downloading a third-party application, then the third party application provider is the entity responsible for providing the appropriate notice and obtaining the appropriate consent to use the location data – not the

[25] Consumers have the ability to decline certain solicitations delivered through email or telemarketing phone calls, and can choose to have their names removed from many direct marketing lists. *See* Preliminary Staff Report at 57 n.139.

[26] *See id*. at 58-59.

wireless carrier.[27] This guideline was established because the wireless carrier or platform operator may or may not have access to the data, and should not have to seek an additional layer of consent from the consumer.[28] Equally important, bombarding consumers with duplicative requests for choice decisions disrupts the user experience and creates confusion.

C. The Implementation of Industry's Self-Regulatory Program for Behavioral Advertising Should Be Given an Opportunity to Work Before the FTC Recommends an Alternative "Do Not Track" Mechanism.

Verizon appreciates Staff's acknowledgment that progress has been made with regard to notice and choice mechanisms for online behavioral advertising. These efforts demonstrate what can be achieved by industry participants who commit to improving privacy practices and why robust self-regulation in the form of policies, best practices, and enforceable industry-developed guidelines should be given a chance to work before other alternatives are considered.

For example, in response to the FTC's recommended best practices for online behavioral advertising, a broad representation of the Internet advertising ecosystem[29] is

---

[27] *See* CTIA Guidelines, Section 2: where a wireless carrier provides user location information to an application developer for use in the application developer's location-based service application that the developer offers through an application storefront, the wireless carrier is not the location-based service provider responsible for providing the required notice and choice.

[28] Of course, if the third-party application provider has contracted with the carrier to obtain the location data on behalf of the third-party application provider, then best practices should dictate that the carrier obtain appropriate assurances from the third party that the user has consented to the sharing of the location data. *See* American Ass'n of Advertising Agencies, et al., "Self-Regulatory Principles for Online Behavioral Advertising," http://www.iab.net/media/file/ven-principles-07-01-09.pdf (July 2009) ("Self-Regulatory Principles").

[29] *See* "Welcome to the online home of the Self-Regulatory Program for Online Behavioral Advertising," http://www.aboutads.info/. The program addresses the principles set forth in the "FTC Staff Report on Self-Regulatory Principles For Online Behavioral Advertising," http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (Feb. 2009).

now actively implementing a comprehensive set of Self-Regulatory Principles for Online Behavioral Advertising.[30] This regime, which covers thousands of different firms involved in online behavioral advertising, establishes specific requirements for entities that collect, use, or share data for online behavioral advertising purposes. Advertisements delivered using online behavioral advertising techniques will carry a uniform icon that leads to a consistently-worded notice about the ad and the information used to deliver it, as well as a mechanism for the consumer to opt-out of the ad campaign and any similar campaigns from participating firms.[31] The program also includes accountability and enforcement mechanisms to ensure compliance. Verizon was an active participant in the development of these principles and is now deploying the icon and consumer notice provisions that the principles set forth on applicable Verizon advertisements. Verizon supports expanded uses of the icon and its connected notice, choice, and education components as well as mechanisms that make the choice decision durable. Notably, these self-regulatory principles, especially with regard to the use of a universal icon, are unique in providing a consistent user experience across the advertising ecosystem. They target the precise data use activity that is the focus of Staff's proposed Do Not Track mechanism.

The online behavioral advertising self-regulatory efforts demonstrate the seriousness with which industry takes the FTC's call for additional consumer options in this area. Industry has invested time, capital, and resources into these practices in an

[30] "Self-Regulatory Principles for Online Behavioral Advertising," http://www.iab.net/media/file/ven-principles-07-01-09.pdf (July 2009) ("Self-Regulatory Principles").

[31] "CLEAR Ad Notice," http://www.iab.net/media/file/CLEAR_Ad_Notice_Final_20100408.pdf (April 2010).

effort to provide consumers with the information they need to make informed choices about the use of their data. Therefore, recommending the establishment of a Do Not Track mechanism is premature. Instead, the FTC should first allow industry to gain experience under the self-regulatory efforts described above.

Moreover, there are several questions about Staff's proposed Do Not Track mechanism that must be addressed to avoid unintended consequences. *First*, Staff's proposed Do Not Track mechanism is an HTTP header extension, which is a browser-based means of communicating a user's tracking preferences. If Web usage tracking methods are developed that do not occur directly through the Web site, HPPT header extension methods will not work. Applications other than Web browsers are numerous and widely used on wireless devices and carry unique user interfaces and protocols that do not always use HTTP to communicate. Where HTTP is not the communication format, the device protocols would have to be revised or extended to carry the equivalent information to the envisioned browser header. These changes may be technically possible, but they will be difficult to implement across industry segments, as there are far more mobile application software developers than there are browser and Web server software developers.

Second, Web sites and third parties must abide by the header extension; otherwise, the header extension will not prevent tracking. Absent a clear definition of what constitutes tracking for purposes of the Do Not Track mechanism, the Web sites expected to abide by the header extension will necessarily have the discretion to determine which practices do or do not constitute tracking. As a consequence, Web sites

could fail to honor users' tracking preferences. These issues are further confounded by the fact that today's Internet ecosystem is global.

The existing cross-industry effort to provide consumers with the ability to opt out of online behavioral advertising uses of their Web browsing data through a uniform icon experience is already being implemented. That icon should be given an opportunity to work before alternatives are considered.

IV. Companies' Data Protection Practices Should Be Transparent.

The FTC's hallmarks of a transparent commercial data use policy – providing notifications and choice mechanisms in easily accessible locations, enabling consumers to compare data practices across companies, providing consumers with reasonable access to their data, disclosing changes to data policies and obtaining consent where necessary, and educating consumers about commercial data practices and the choices available to them – can guide the development of industry best practices in this area. For example, privacy seal programs such as those administered by TRUSTe and BBBOnline require Web sites that hold the seals to incorporate the privacy best practices associated with these programs. Also, as discussed earlier, the Self-Regulatory Principles represent a comprehensive effort to establish user-friendly practices for online advertising across the Internet advertising industry. Education, transparency, consumer control, and accountability are among the principles that guide the program. In addition, the CTIA Guidelines incorporate notice and consent principles that dovetail with the FTC's goals for increasing transparency. These self-regulatory efforts should form the backdrop against which the FTC finalizes its framework for increased transparency in commercial data use policies.

For example, Staff recommends that companies "should standardize the format of their notices, as well as the terminology used."[32] While streamlined and standardized notices and terminology can prove useful to consumers and practical for companies to implement in particular contexts like the online behavioral advertising in-ad notices, standardized notices are less practical in other circumstances – either because critical information may have to be excluded from the notice in order to make it fit the "standard," or because visual displays on a device do not lend themselves to displaying certain notices in a form that consumers can reasonably be expected to manage. The CTIA Guidelines "do not dictate the form, placement, terminology used or manner of delivery of notices" for location-based services.[33] Rather, those guidelines emphasize that notices "must be provided in plain language and be understandable."[34] The wireless industry has advanced data practice transparency by refining notices so that they provide consumers with critical information in digestible form and facilitating consumers' ability to navigate to dashboards or other locations where additional, less critical information can be obtained.

Staff's recommendations regarding consumer access to data must be carefully considered with regard to the data involved, the feasibility of providing such access, and the consumer benefit such access might provide. Verizon agrees with Staff that a consumer's ability to access data held by a company should depend on the sensitivity of the data and its use.[35] Consumer access to data is far more important where that data is

[32] Preliminary Staff Report at 71.

[33] CTIA Guidelines at 3.

[34] *Id*.

[35] Preliminary Staff Report at 73.

used to make decisions, such as in the credit reporting context, than where data is not used to make a decision affecting the consumer. There are significant costs and technical challenges associated with providing access to data in a manner that would be meaningful to consumers. Verizon agrees that a reasonable middle ground may be to ensure that consumers have access to their *elections* about data usage, rather than access to the data itself.[36] Consumer access to choice settings enables them to control the manner in which data is collected and used and mitigates the need for direct data access. It also avoids the significant expense associated with creating methods that allow consumers to access data other than typical account-related information. Otherwise, it is highly likely that companies could expend – and waste – significant resources creating elaborate data access measures that few consumers actually utilize.

CONCLUSION

Verizon shares Staff's commitment to the protection of consumer privacy and applauds Staff for developing a framework that carefully considers the appropriate ways in which to protect consumer data privacy interests amidst the stunning success story that is the Information Age. Verizon urges Staff to continue to support and encourage ongoing industry self-regulatory efforts and to allow those self-regulatory initiatives to proceed and mature before recommending alternatives. Verizon is confident that the final report will empower responsible industry members to continue in their privacy protection efforts, encourage absent members to join the rest of the industry in adopting privacy

[36] Preliminary Staff Report at 75 n.175 (noting efforts by eBay and Google to provide consumers with access to their data and tools to suppress or otherwise control the information).

practices that ensure the responsible handling of consumer data, and maintain the effective balance between privacy protection and digital economic growth and prosperity.

Respectfully submitted,

Kathleen G. Zanowic
Chief Privacy Officer
VERIZON
1320 North Court House Road, 9th Floor
Arlington, Virginia 22201
(703) 351-3156

Karen Zacharia
Magnolia Mansourkia
Jamellah Ellis
Christopher Oatway
VERIZON
1320 North Court House Road, 9th Floor
Arlington, Virginia 22201
(703) 351-3199

John T. Scott, III
VERIZON WIRELESS
1300 I Street N.W., Suite 400 West
Washington, DC 20005

February 18, 2011