mozilla

February 23, 2011

Federal Trade Commission
Office of the Secretary
Room H-135 600
Pennsylvania Avenue
Washington, DC 20580

RE: Federal Trade Commission (Bureau of Consumer Protection) A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers

Dear Mr. Secretary:

Mozilla submits these comments in response to the December 1, 2010 Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Choice: A Proposed Framework for Business and Policymakers," regarding how best to protect consumer privacy while supporting beneficial uses of information and technological innovation.

Mozilla supports the FTC's proposed framework as an improvement to existing models and believes its adoption will further enhance public trust and confidence in the market, as well as foster support for new web-based innovations in privacy-enhancing technologies.

We are particularly appreciative of the process undertaken to engage the public throughout the past year and through the FTC's ongoing efforts to solicit input from industry stakeholders and the public on its preliminary report.

On behalf of Mozilla, we thank you for the opportunity to comment on the proposed framework. Please do not hesitate to contact us with any questions or for additional input.

Respectfully Submitted,

/s/

Alexander Fowler
Global Privacy and Public Policy Leader
Mozilla
650 Castro Street, Suite 300
Mountain View, CA 94041
(650) 903-0800, ext. 327

mozilla

Comments on A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers

Prepared by Mozilla and Submitted on February 23, 2011

We applaud the FTC in seeking public input to rethink prevalent formulations of privacy and explore new models for providing consumers with adequate and meaningful choices and controls over their online and offline interactions.

In response to the FTC's call for input on its proposed framework, we respectfully submit our comments, which are summarized as follows:

- Mozilla supports efforts to broaden the definition of personal information to data that can be reasonably linked to a specific consumer, computer or device. We recommend that the FTC look to industry best practices in the area of data classification for other models of defining personal information, and we point to the emergence of browsing history, geolocation, behavioral advertising data, browser fingerprints, and the social graph as examples of personal information that warrant additional consideration.
- The lack of industry best practices, standardization and technology tools related to Privacy By Design may lead to undue burden on consumers to make sense of the emergence of hundreds of similar privacy configurations across the web.
- Mozilla supports a full range of innovations and industry practices that enhance consumer choice and control with regard to online behavioral advertising, including the creation of a uniform and comprehensive choice mechanism through a new Do Not Track (DNT) HTTP header as another step in the evolutionary arc of privacy improvements. Continued FTC leadership is required to develop consensus on the scope of DNT as it relates to online behavioral advertising and implementation across the online advertising industry.
- We support efforts to improve online privacy policies and notices, such as graphical icons as one technique, in conjunction with other mechanism like contextual notices, which simplify the consumers' ability to quickly understand and act on an organization's data handling practices.

I. Introduction

Mozilla is a global community of people working together since 1998 to build a better Internet. As a non-profit organization, we are dedicated to promoting openness, innovation, and opportunity online. Mozilla and its contributors make technologies for consumers and developers, including the Firefox web browser used by more than 400 million people worldwide. As a core principle, we believe that the Internet, as the most significant social and technological development of our time, is a precious public resource that must be improved and protected.

Privacy and security are important considerations for Mozilla. They are embraced in the products and services we create, and derive from a core belief that consumers should have the ability to maintain control over their entire web experience, including how their information is collected, used and shared with other parties. We strive to ensure privacy and security innovations support consumers in their everyday activities whether they are sharing information, conducting commercial transactions, engaging in social activities, or browsing the web.

There are many challenges in both practice and theory that face organizations when it comes to privacy. These range from compliance with a non-uniform set of global regulations to supporting a broad spectrum of people's privacy values to definitional issues that together introduce friction into much of the discourse around privacy. In some respects, these challenges have had a chilling effect and led to the exact opposite of the transparency, choices and innovations that are required in this area.

Even when the topic of privacy is discussed, as the FTC roundtables highlighted, inconsistent nomenclature often thwarts meaningful dialogue among informed stakeholders. Privacy means different things to different parties. It is often contextual and what is viewed as appropriate varies based on the specifics of the transaction and consumer expectations. Some differences are definitional, such as agreeing on what constitutes personally identifiable information (PII). Today, even this definition can differ depending on jurisdiction, not to mention that PII can be derived from many seemingly non-PII bits and pieces of a consumer's data and activities.[1]

[1] "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," Paul Ohm, University of Colorado Law Legal Studies Research Paper No. 09-12, August 13, 2009; http://ssrn.com/abstract=1450006

Other differences are more structural and derive from different values. See for example, James Whitman's analysis of transatlantic privacy practices and cultures in *Two Western Cultures of Privacy*,[2] suggesting the roots of European privacy protections derive from values rooted in controlling one's presentation versus American privacy notions rooted in the protection against government intrusion. This is just one vector that begins with different values and concludes with different outcomes. Introduce other values like user experience, commercial objectives, and/or constraints provided by form factors and the scope of the privacy challenge is further expanded.

Mozilla navigates these varied definitions and values by focusing on the central belief that the web should be open, innovative, and consumers should have meaningful choices. In this context a simple formulation of our goal is to allow the consumer to control his/her own information and how it is shared and disclosed. However, this does not mean the consumer should never disclose information.

A major facet of the web is that it leverages user data to enable a rich ecosystem of services and features. This does not mean consumers should have to affirmatively opt into every collection or use of information, however. An open web that supports meaningful choices also recognizes that the Internet inherently operates best with some, select disclosures of information being seamless; and consumers accept this as normal on the web provided they can, if and when they want, make informed decisions about how and when data is collected, used and/or shared.

II. Getting Beyond PII/Non-PII

A. Mozilla supports broadening definitions of personal information to include data and combinations of data that may be reasonably linked to a specific consumer, computer or device.

To a certain extent, much of the data collected from a consumer online could be reasonably considered personal by that person. Whether data is uniquely identifiable or becomes identifiable in combination with other data, or whether future, novel uses of that data create new contexts with privacy properties, people can have legitimate interests in wanting to understand

[2] *Yale Law Journal*, Vol. 113: 1153

and have a say in an entity's data handling practices. The roundtables and FTC's preliminary report highlighted a number of examples, including data aggregation of anonymous or de-identified user data, browser fingerprints, unique device identifiers on mobile devices, geolocation data, and online behavioral tracking data for advertising.[3]

As a byproduct of fundamental web topology, a number of data elements are created, often referred to as digital exhaust,[4] which may have privacy attributes alone or in combination with other data. Today, this data may be used for unintended purposes that are beyond consumer expectations and lack transparency and/or accountability. Input from the FTC on how its proposed framework would apply in these instances would be helpful.

Further, as we considered additional examples for the FTC to consider of how new forms of linkable, non-PII continue to emerge and create potential privacy concerns for people online we encourage more discussion on data about the sets of relationships people maintain online, which is also referred to as the social graph.[5]

Every desktop operating system, and hundreds of web-based service providers, has some way of representing the social graph or "who you know." Mozilla believes that the compilation of a consumer's online relationships into a digital object has a number of similarities to other forms of personal information, that could be considered "personal" in the minds of many consumers despite the common appeal of some social networks.[6,7]

Uses of the social graph today include a growing list of activities with consumer protection-related facets, including both first party and third party marketing, fraud detection, employment decisions and financially-related determinations like credit scores. The social graph is a core innovation driving the development of novel, fun and important web applications and services today, and the list of applications of the graph will continue to expand. There are, of course, illegitimate uses of the graph by hackers and identity thieves that warrant the FTC's full attention, however, from a privacy perspective, the focus here is on legitimate uses of the graph that consumers may still want to have a greater understanding about. The privacy concern is

[3] Prelimminary FTC Staff Report, pp. 36-37
[4] See http://en.wikipedia.org/wiki/Digital_exhaust#cite_note-digital_exhaust_1-0
[5] "Explaining what the 'Social Graph' is to your Executives," Jeremiah_Owyang, November 10, 2007; http://www.web-strategist.com/blog/2007/11/10/what-is-social-graph-executives/
[6] "Pulling back the curtain on 'anonymous' Twitterers," Nate Anderson, *Ars Technica*, March 31, 2009; http://arstechnica.com/tech-policy/news/2009/03/pulling-back-the-curtain-on-anonymous-twitterers.ars
[7] "Eight friends are enough: social graph approximation via public listings," Joseph Bonneau, et al., *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, ACM, 2009, pp. 13-18

that these new practices sometimes outpace people's ability to understand all of the uses and potential pitfalls. As a result, we think additional discussion and study in this area would be beneficial.

B. It is time to rethink the way in which personal information is defined. The FTC should look to industry best practices in the area of data classification for other models of defining personal information.

To consumers, as was stated above, many types of personal information can be important, including elements that are uniquely identifiable or not. Meaningful distinctions between PII and non-PII are breaking down, as the example of the social graph illustrates. However, other ways of defining personal information exist, as evidenced by the decade plus experience IT organizations within the public and private spheres have had with data classifications. The technical literature is rich in various classification schemes, taxonomies, models, and best practices for applying varying levels of privacy and security to specific data elements.[8] We encourage the FTC to review some of this literature. For instance, the National Institute for Standards and Technology has provided guidance to the federal government for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability,[9] while many IT control frameworks provide additional models of classifications for the private sector.[10] The primary advantage of moving away from PII/non-PII to multi-tiered classification schemes will be enhancing organizations' ability to define data types and controls based not only on sensitivity, but also in conjunction with vulnerability and threat information to better manage risk to an organization and ultimately provide meaningful protections to the consumer.

III. Privacy By Design in an Online Ecosystem

A. Privacy By Design (PBD) is a powerful concept but it must be accompanied by further definition, industry best practices, and some standardization to avoid undue burdens

[8] Understanding Data Classification Based on Business and Security Requirements," Rafael Etges and Karen McNeil, *Information Systems Control Journal*, 2006

[9] "Standards for Security Categorization of Federal Information and Information Systems," Ross, R. S.; Swanson, M., February 01, 2004; http://www.nist.gov/customcf/get_pdf.cfm?pub_id=150439

[10] See the "COBIT Framework for IT Governance and Control," ISACA; http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

on consumers trying to make sense of hundreds of different privacy configurations across the web.

PBD is a worthwhile endeavor and one that is core to Mozilla's mission. Mozilla recently promulgated a series of design and operational principles that were the outcome of a series of open dialogues among Mozilla's broader community.[11] As we look to extend internal controls over our own data handling practices for our consumers and employees, develop new products and services, and work with service providers and partners, the principles are helpful to guide decision-making and consider privacy and security as key components to our many activities and products. This is one example of how organizations can build upon the PBD recommendations being made by the FTC and translate them into practical tools within the organization.

Another example of PBD at Mozilla is Firefox Sync, our cloud-based service for Firefox users to continuously synchronize bookmarks, browsing history, saved passwords and tabs across multiple PCs and mobile devices.[12] Firefox Sync encrypts user data on the computer and uploads encrypted consumer data over the network using SSL communication. Only the user has the ability to access his/her sync data via a secret passphrase, and the user has complete control over its use, including sharing of that data with others. Mozilla provides the cloud-based storage, but we are technically unable to view users' stored passwords and browsing history. This exemplifies how it is not only technically feasible, but also enriching to design privacy and security into the cloud. These same protections could apply to other cloud storage providers without business interests in secondary uses of consumers' personal information stored on their servers.

The FTC's proposal makes sense within an organization, where the design, develop and deploy process[13] is largely within an entity's control and a broad spectrum of privacy-related values could be considered throughout the process. However, in the context of the web, where different entities with unique development lifecycles and business models compete for consumers, PBD in practice becomes more complex and may present some challenges that need to be considered in the context of the FTC's proposed framework.

[11] See https://firstpersoncookie.wordpress.com/2011/01/12/mozillas-draft-privacy-data-operating-principles/
[12] See http://www.mozilla.com/en-US/mobile/sync/ and https://wiki.mozilla.org/Labs/Weave/Crypto
[13] It is worth remembering that for PBD to be a meaningful exercise, the requirements defined during the design phase need to be successfully carried through development and deployment phases to ultimately provide value to the consumer.

Different sites and services are in the process of designing variations of the same configurable privacy points across the web. For example, the number of configurable privacy settings within one prominent social network received significant public attention last year, which pointed to consumers having to review 50 settings with more than 170 options.[14] While this site and others like it are putting PBD into action, confusion caused by the complex set of privacy options as a whole may dramatically reduce the effectiveness of various privacy features. PBD may not be enough unless it results in something consumers can identify and understand coherently across products and services.

It is certainly possible that many other organizations will replicate this example as the FTC's framework is adopted across the industry. However, amplifying this to the many places where consumers set and reset the same preferences across sites and services, PBD in practice could end up in a similar place to where the industry is now with overly complex and consumer-unfriendly online privacy policies. The result may be that preferences end up not being uniformly expressed, in some cases, or inconsistently configured in other cases. And the burden of managing privacy configurations across multiple sites, services and devices will fall to consumers and even then only to the likely few who take the time to understand each implementation and its tradeoffs.

There needs to be more thought given to how to design common choices and configurable points for privacy to realize the full potential of PBD. More development in best practices is also necessary for contextual notices and actions that happen at the point of data collection and sharing, as well as technical ways to bound preference elections to specific times and transactions.

The broader societal importance of preserving privacy and enhancing consumer choice and control online, which transcend business models and technology platforms, should drive those on the forefront of PBD to openly share best practices, technical implementations and tools to the broadest community of developers and consumers. This is an area where the FTC could assist in convening industry stakeholders to flesh out more of the details of what PBD means in practice.

[14] "Price of Facebook Privacy? Start Clicking," Nick Bilton, *New York Times*, May 12, 2010; http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html

IV. Do Not Track Mechanisms for Online Behavioral Advertising

A. Mozilla supports browser, advertising and web site innovations that enhance consumer control and choice with regard to online behavioral advertising (OBA).

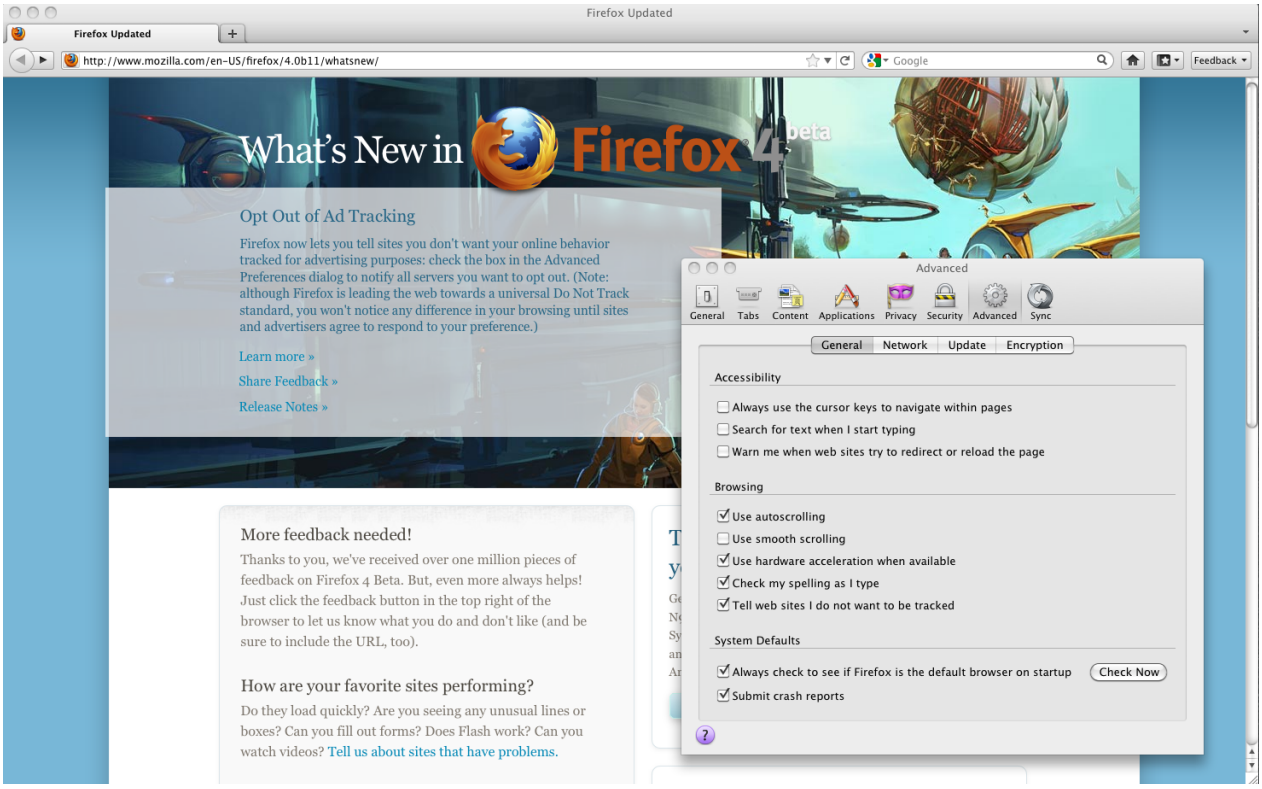
Unlike blocking lists or opt-out cookies, which place the burden on the consumer and, more importantly, do not respond to all forms of OBA-related tracking and targeting, a DNT header has the potential for consumers to broadcast preferences for advertisers and publishers to honor while not undermining or blocking all forms of advertising. Success of the header approach will require support and collaboration from stakeholders across the display ad ecosystem. Continued FTC leadership will also be necessary to establish consensus within the industry on the scope and implementation of DNT.

Since the release of the FTC's proposed framework, there has been considerable public and media attention given to the topic of online behavioral advertising (OBA) and the FTC's recommendation for the creation of a Do Not Track (DNT) mechanism. Mozilla recently added the new HTTP DNT header that Firefox users can use to state a preference to not be tracked across websites for advertising, which will co-exist with other browser-based privacy and cookie-based tools already available to Firefox consumers today.[15,16,17]

The DNT header builds on the work of the advertising networks without the cookie-based systems they make available to people online. There are many advantages of the header technique over the cookie-based technique; it is less complex and simple to locate and use, it is more persistent than cookie-based solutions, it addresses all forms of OBA-based tracking that may not all be cookie-based, and it does not rely on consumers finding, loading and managing lists of ad networks and advertisers to work.

[15] "More Choice and Control Over Online Tracking," Alexander Fowler; https://firstpersoncookie.wordpress.com/2011/01/23/more-choice-and-control-over-online-tracking/
[16] "Opting-out of Behavioral Ads;" Sid Stamm; http://blog.sidstamm.com/2011/01/opting-out-of-behavioral-ads.html
[17] "Thoughts on Do-Not-Track," Michael Hanson; http://www.open-mike.org/entry/thoughts-on-do-not-track

Screenshot: Firefox Welcome Page with Configuration Panel Open to Show DNT Header



However, it is important to point out that browser implementation of the DNT header does not represent a complete solution, as industry participation is required to create the technical mechanisms to respond to DNT browser requests broadcast by consumers via their browsers.

A number of ad networks, advertisers and publishers are very supportive of the DNT header and see it as preferable to cookie-based or list blocking approaches. Consensus is emerging that a simple first step for responding to a consumer's intent could be: if the DNT header is present and the site or third-party advertiser has a tracking opt-out mechanism, then the mechanism should be activated. If the site or third-party advertiser does not have an explicit opt-out mechanism, the consumer should experience only content from a first-party relationship with the page being viewed. For behavioral advertising servers and data brokers, the intent of a DNT header is quite clear: it should be interpreted as though the consumer visited the opt-out registry and clicked the checkbox and that the consumer's activity or data is not collected or logged. We expect announcements to be forthcoming shortly on how first party and third party entities will be responding to the DNT header.

B. The FTC Should Seek Ways to Accelerate the Process of Industry Adoption of the DNT Header

There are a number of steps ahead that will require continued leadership and support from the FTC to see companies implement responses to consumers with the DNT header enabled, including:

- Fostering consensus on what the DNT header means to all stakeholders. We have proposed an initial definition focused on the display advertising market, and we seek a focused definition all stakeholders can agree upon.
- Helping to educate the public on DNT and what reasonable expectations of privacy people should have when using the DNT header or other mechanisms in a browser.
- Working with sites, advertisers and data brokers to establish best practices in implementing meaningful responses to a DNT header that are transparent to the public.
- Evaluating enforcement mechanisms to combat entities that systematically ignore the DNT header and jeopardize those efforts made by responsible companies.

We are currently working with several companies, and academic and public interest groups to bring a technical proposal to the IETF for the DNT header. However, by moving the discussion from a technical domain to a policy domain, the FTC can help to accelerate the process of evaluating the merits and implementation requirements of the DNT header.

Gathering feedback from the technical community is necessary, but another important step will be to validate the merits of the scheme with legal and regulatory experts. In actual practice, a DNT header could be an important piece of a consumer protection scheme. By creating a clear statement of consumer intent, the header could allow a regulatory body to investigate claims of improper data usage. If an organization was found to track consumers in spite of the presence of affirmative DNT headers, and after a reasonable length of time for implementation had elapsed, a stronger case could be made that they were infringing consumers' privacy. This obviously does not work for sites that ignore consumer intent or break laws; stronger technical countermeasures will be necessary in those cases.

V. Seeking New Ways to Improve Transparency of Data Practices

A. We support efforts to improve online privacy policies and notices that simplify the consumer's ability to quickly understand and act on an organization's data handling practices. Advances in mobile platforms and web applications create opportunities to break from traditional, legalistic privacy policies, which in turn may provide new models for improving more standard web privacy policies.

A Do Not Track HTTP header for online behavioral advertising is only one piece of the data choice and control privacy puzzle. Improving transparency into online data collection and sharing practices is another area where we think there is room for improvement and innovation.

In 2010, Mozilla convened a workshop that brought together some of the world's leading thinkers in online privacy to answer the question: what attributes of privacy policies and terms of service should people care about? The workshop resulted in a refined set of definitions for a series of graphical, icons to enhance consumers' ability to understand and act on privacy notices. The work was later presented to the W3C as a model approach for broader discussion.[18]

As the FTC report highlighted, privacy policies and terms of services are often complex, legalistic documents that encapsulate a lot of situation-specific information that can be difficult for people to understand and act on. The web supports myriad business, communication, technology and data practices that ultimately need to be explained in a privacy policy, making it difficult to reduce these consumer notices to standardized boilerplate or even accessible content.

Taking a cue from The Creative Commons, which uses a set of icons to help people visually communicate copyright preferences when sharing content online, we set out to design a series of icons that could make it easier for people to understand privacy policies and act on them in a real-time basis while interacting with a web site or company online. Mozilla recently blogged about our latest set of privacy icons, which cover the following key attributes:[19]

[18] W3C Workshop on Privacy for Advanced Web APIs, July 12-13, 2010, London; http://www.w3.org/2010/api-privacy-ws/report.html
[19] See http://www.azarask.in/blog/post/privacy-icons/

- Is data used for secondary use? And is it shared with 3rd parties?
- Is data sold or bartered?
- Under what terms is data shared with the government and with law enforcement?
- Does the company take reasonable measures to protect data in all phases of collection and storage?
- Does the service give consumers control over their data?
- Does the service use data to build and save a profile for non-primary uses?
- Are ad networks being used and under what terms?

Figure: Example Privacy Icons

Your Data May be Used for Purposes You Do Not Intend

Your data is never bartered or sold.

Without delving into the specifics for each icon, there is merit in the idea that everyday consumers can glance at simple icons within a form, at the bottom of an email, or within a privacy policy and know if and how their data may be used. At the same time, these icons can provide a wide range of organizations with the flexibility to create comprehensive and meaningful policies that reflect the complexities of their business.

Mozilla is in the process of further refining the icons and considering ways to begin experimenting with them online. An initial idea is that privacy icons may prove highly effective for web applications, widgets, microsites, web demonstrations and mobile sites where long, text based policies are difficult to render, read and often detract from the consumer's experience. In addition, we may refocus the icons to cover data handling practices that fall outside of the definition of commonly accepted practices discussed within the FTC report.

As with all of our work, we will continue to seek public input on our approach, as well as share the results of our experiments widely.

VI. Conclusion

Mozilla supports the FTC's proposed framework as an improvement to existing models and believes its adoption has the potential to further enhance public trust and confidence in the

market, as well as foster support for new web-based innovations in privacy-enhancing technologies. In fact, the FTC's recommendations have broad utility beyond only commercial activity and would improve people's choice and control in the full range of interactions they have with public and private entities. We encourage non-commercial entities, including non-governmental organizations, educational institutions, and state, local, and federal agencies, to consider how the FTC's proposed framework applies to their data handling practices.

On behalf of Mozilla, we thank you for the opportunity to share our perspectives on this important topic.

VII. Contact

Please direct questions and/or comments to:
Alex Fowler, Global Privacy and Public Policy Leader, Mozilla
650 Castro Street, Suite 300, Mountain View, CA 94041 (650) 903-0800, ext. 327