Via electronic filing

February 18, 2011

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Comments on the Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change

Dear Secretary Clark,

Thank you for the opportunity to comment on the recently released interim report entitled *Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Report). Yahoo! appreciates the hard work the Commission is doing to evaluate practices for the myriad data usage models present in the marketplace today, as well as the opportunity to comment on aspects of the Framework proposed by the Commission.

Yahoo! has been focused for more than a decade on balancing the demand for more innovative and personalized online services with the need to protect personal privacy. From the company's earliest days, we have worked to integrate privacy notices and tools into our products from their inception, placing Yahoo! in a unique position to offer input on the proposed framework and to answer your critical questions.

Yahoo! is the premier digital media company. Founded in 1994 by Stanford PhD candidates David Filo and Jerry Yang as a way for them to keep track of their personal interests on the Internet, Yahoo! has grown into a company that helps people navigate the vast expanse of information, find the best of the Web, more easily discover what they are looking for — and perhaps discover something new.

Today, we're a leading global brand that uses technology, insights, and intuition to deliver customized digital experiences. We give consumers across the globe simple, trusted ways to connect with the people, communities, topics, and trends that matter to them most. We attract more than half a billion consumers every month on every continent in more than 30 languages — making Yahoo! one of the most visited and most trusted Internet destinations. Yahoo! changed the way people communicate, learn, discover, connect, shop, share, and conduct business. Our business focus is on creating a content, communications, and community platform that delivers rich consumer experiences and advertising solutions across the screens of people's lives —from desktops to mobile devices, from tablets to connected TVs — all around the globe. Yahoo! is headquartered in Sunnyvale, Calif., and has more than 13,000 employees in 25 countries, provinces, and territories.

It is no coincidence that the U.S. is the birthplace of many of the most widely used global websites and online services. U.S. legal frameworks encourage innovation through reasonable liability regimes, controls on harmful uses of information, promotion of a diversity of online voices, security requirements based on the sensitivity of the data, and a light regulatory hand that favors and recognizes complementary roles for industry self-regulation. Further comments on these ideals are embedded in our response to specific elements of the Framework outlined by the Commission below.

The Commission notes that, "in developing the proposed framework, staff was cognizant of the need to protect consumer privacy interests effectively, while also encouraging the development of innovative new products and services that consumers want."[1] The Department of Commerce, in its recently released Green Paper also reflects this view as it acknowledges the "United States' dual emphasis in commercial data privacy policy: promoting innovation while providing flexible privacy protections that adapt to changes in technology and market conditions."[2] As a company dedicated to bringing consumers the innovative and personalized products and services they increasingly want, Yahoo! encourages the Commission to continue to affirm that effective privacy protections can and should take place in a manner that allows innovation to thrive.

1. Scope of Data

At the outset of its Report, the Commission redefines the scope of entities and data to be covered by its proposed privacy framework as "all commercial entities that collect or use consumer data that *can be reasonably linked to a specific consumer, computer, or other device*." This scope of data includes basic non-personally identifiable data collection or use that facilitates the free flow of information across the Internet, and is therefore a significant departure from the types of data

[1] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 39.

[2] "*Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*" The U.S. Department of Commerce. Internet Policy Task Force. 16 Dec. 2010. <http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf>..at p.vii

traditionally regulated within the U.S. Several well-established domestic privacy laws instead constrain the use of "personally identifiable information", (PII) under certain conditions. Further, privacy policies and established internal procedures have been predicated on and implemented by reviewing the use of data sets that specifically identify users in areas such as name, address, social security number and the like. Indeed, while the scope of the PII definition may vary among sectoral laws, it almost always requires a connection to a specific physicial individual (which certainly could include online identifiers like email).[3] Yahoo! believes there is no justified basis for a departure from this historical treatment of PII in the regulatory context and doing so could have the unintended consequence of resulting in more harm than good, even though intended to protect consumer privacy.

The Commission notes a key theme stemming from the series of Roundtables held in 2009 and 2010 is the "decreasing relevance of the distinction between PII and non-PII."[4] There have been occasions where researchers have been able to re-identify some data sets in ways that were not tested in the past, as mentioned in the Report. However, a blurring of the distinction between PII and non-PII does not mean there is *not* one, or that such distinctions are not *relevant*. Yahoo! believes that information that falls outside of the traditional PII categories does not pose the same privacy concerns for consumers and, further, many companies have gone to great lengths and incurred substantial costs to address residual privacy concerns by anonymizing or de-indentifing data.

Data that is NOT linked to personal identifiers is not the same, and should not be treated the same, as data that *are* directly linked. In trying to address the circumstances in which traditional non-PII is linked to PII, the Commission's definition would cover non-PII data in all cases. This overbroad definition will not enhance consumer privacy and would appear to act as a disincentive to incurring the cost and effort otherwise required to hold data in non-identifiable forms. Companies have come to rely upon established notions of the distinctions between PII and non-PII, and have therefore voluntarily undertaken many measures to hold only the data they need in identifiable form and to de-indentify as much as possible subject to legitimate business needs. In addition, it is not clear what the addition of the qualifier "reasonably" to the notion of "linking" would accomplish that would yield a benefit to consumer privacy. For instance, if linking is possible but is against the policies of an entity, but would now be covered data simply because it is held by the same entity (and could therefore potentially be reasonably linked), there would be an apparent disincentive to hold data in non-identifiable forms. In other words, data are more likely to be linked in practice if regulation suggests it is covered even when pains have been taken to maintain it as non-PII. This is an important consideration for the Commission as it

[3] See for example, Health Insurance Portability and Accountability Act regulations, 45 C.F.R. Sections 160.103 and 164.514; Children's Online Privacy Protection Act regulations, 16 C.F.R. Section 312.2, CPNI Provisions of the Communications Act at 47 U.S.C. Section 222(h)

[4] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 35.

reviews answers it receives from others about how to treat data that may be considered linkable in the future.

Further, the Commission suggests linkage to a specific computer or device should be covered in the same way as linkage to a specific consumer. Many computers and devices are used by multiple users, some within households and others within more public spaces such as universities or libraries. In such cases, usage is not tied to a specific individual, which would be more in line with traditional notions of data best suited to privacy regulation.

Yahoo! suggests the more appropriate scope is data that *are* linked to a specific consumer. In this way, online and offline companies would be directed to expend their limited resources to protect the data most likely to result in the kinds of harms and concerns outlined by the interim report. This also has implications for the implementation of key portions of the proposed framework such as Privacy by Design, as noted below.

2. Privacy by Design

Yahoo! supports the concept of Privacy By Design (PBD) for companies, which focuses on the importance of applying privacy considerations throughout the entire life cycle of technologies and procedures, from the early conceptual and design stages through to deployment. This is a fundamental part of how Yahoo! currently develops products and services, and is a critical factor in avoiding serious privacy-related problems. It also plays a central role in making Yahoo! one of the most trusted brands on the Internet[5].

As Yahoo!'s Chief Trust Officer, I oversee Yahoo!'s dedicated privacy and data governance group and its work applying PBD principles to products and services, particularly in a consultative role with the product, engineering and customer care teams. My team actively trains Yahoos about data policies in addition to its product guidance and policy compliance functions. Organizationally, my team is distinct and independent from the legal, public policy and product engineering divisions, allowing each of these respective groups to contribute a complementary point of view to privacy and data governance as a consortium.

At the outset it is important to recognize that each company depending on its size, scale and global footprint will inevitably require a tailored approach to privacy governance within that company. While one size rarely fits all, and therefore prescriptive regulation describing how each company should be internally structured from a privacy perspective is undesirable, the importance of dedicating teams to education and establishing and enforcing PBD principles is reflected in the work of these groups, and demonstrates that PBD can be a successful supportive function to business objectives.

[5] Yahoo! is the #1 most trusted technology brand in the world, a full 13% ahead of the nearest competitor in the technology category. Source: 2010 Edelman Trust Barometer.

2.1 Specific Business Purpose

The Commission suggests that PBD should conceptually include a restriction on collecting "only the data needed for a specific business purpose". Yahoo! agrees that data collection should have a purpose, and we have adopted layered privacy notices to give users specific information about each product we offer and how information is used to provide it.[6] However, the Commission should realize that data used for one purpose is often legitimately used for others in the same general category as well. Log data collected as users peruse our website will be used to provide baseline reporting and analytics, to customize content, to determine which pages and features are working well and which need improvement in construction and/or navigation, to customize advertising, to bill advertisers, to combat fraud and support audit requirements, to detect and defend against security attacks, and for continual research and development of new product and services. Our research labs are constantly researching ways to bring value to our users and our advertisers. These general uses should be disclosed to users, but the cost of being overly-specific about each use of data is that innovation on behalf of users could be unnecessarily encumbered, delayed or limited. Moreover, such disclosures would create longer, highly detailed privacy notices that are difficult for users to comprehend, or users may become numb to repeated disclosures and repeated intrusions on the user experience they desire and expect. Instead, in our experience, disclosing categories of data use is the clearest and most efficient method of being transparent.

As PBD is contemplated for a product, it must be acknowledged that innovative uses of data will sometimes surprise users, even if the surprise is a pleasant one due to the more useful features and functions users receive. Some products should be introduced as innovative and useful even when data are used in ways that may not have been apparent to the user[7]. PBD must be implemented in ways that allow for game-changing technologies so that innovation can meet growing user expectations and demands for more relevant, intelligent experiences. It is this type of innovation that has set United States companies as leaders in the online space across the globe.

To that end, Yahoo! suggests that "specific business purpose" or "need" be defined to cover general categories or purposes that are reasonably foreseeable, but in defining these terms, the Commission take care not to foreclose innovation by implementing restrictions that would limit new and potentially beneficial uses of data. While the FTC proposes that commonly accepted practices do not require consent later in the Report, the burden of

[6] See http://info.yahoo.com/privacy/us/yahoo/products.html.

[7] For example, the Amazon, Pandora or Netflix recommendation engines use data beyond the specific transaction of buying a book, hearing music, or renting a movie.

determining such uses falls on site operators who can ensure compliance only through disclosure.

2.2 Retention Periods

It is unclear that the marketplace is focused on data retention policies. Yahoo! has led the way with one of the most restrictive data retention policies in the industry, addressing calls for minimal retention.[8] Yet customers appear to be indifferent about this policy. Indeed, we hear very little from our customers on this front and think the emphasis on retention may be misplaced.

Businesses have different data needs, so it may be quite easy for some data models to comply with shorter retention periods while it is not for others. It is true that many uses of information in the behavioral advertising context may be naturally time constrained, from a relevance perspective. However, research around long-term effects of various customization techniques may require longer-term use of data in some form. Regulators should expect that the uses and need for data in its various forms will fluctuate over time and across product and user experience needs. As long as a business can justify its business purpose for holding data, it should be permitted to retain the data so long as is necessary to achieve legitimate purposes, given that data remains a crucial building block of the information economy and differentiated innovation.

Rather than focus on retention periods, Yahoo! sees the application of reasonable security practices suggested in the report to be a more important and practical way to protect data, encompassing the recognized distinction among data types based on sensitivity now well-recognized by existing Commission guidance.[9]

2.3 Data Accuracy

Data Accuracy is an important attribute of systems that use data for decisions that implicate potential adverse impacts on users, such as unfavorable credit determinations or negative employment decisions. Such systems use data in a manner that should be contrasted with, for example, marketing data. The Fair Credit Reporting Act applies to data that has "a bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" when it "is used or expected to be

---

[8] Yahoo!'s Data Anonymization Policy includes the shortest retention period announced by any large search provider at 90 days for most web logs with limited exceptions to fight fraud, secure systems and meet legal obligations.

[9] The report indicates companies "should employ reasonable safeguards – including physical, technical, and administrative safeguards" and "the level of security required should depend on the sensitivity of the data, the size and nature of a company's business operations, and the types of risks a company faces." "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 44-45.

used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes or employment purposes."[10] These are serious issues, with serious consequences, and simply do not compare to data that suggests whether or not a consumer is interested in automobiles. Therefore, the Commission's guidance that companies "should take reasonable steps to ensure the accuracy of the data they collect" is helpful, if the term "reasonable" is applied as it has been in the security space.[11]

Notwithstanding the differences between PII and non-PII, which we believe has fewer privacy implications, Yahoo! has taken an holistic approach to transparency for its interest-based advertising categories through our Ad Interest Manager Product. Yahoo! launched Ad Interest Manager, or AIM in December 2009, which allows users to see what standard interest categories they are placed in for interest-based advertising purposes.[12] AIM also allows consumers to see the types of data that contribute to those categorizations, and to opt-out of specific categories or all interest-based advertising. Because Yahoo! provides visibility into this type of data, users can also "correct" or make Yahoo!'s understanding of their marketing preferences more "accurate". This is a reasonable and proportionate approach to accuracy that does not require FCRA levels of effort.

Because we allow users to access their profile and registration information at any time, Yahoo! does not try to ensure the accuracy of users' full registration information. Registration information is self-reported data, and is not used for critical decisions such as those regulated by the FCRA. It would be costly, time consuming, and actually contrary to privacy objectives for Yahoo! to seek to verify and maintain full and accurate information on registration information such as gender, age or hometown. Yahoo! believes this approach is a reasonable and proportionate way to interpret the Commission's guidance in this area.

2.4 Legacy Data Systems

In response to the Commission's question regarding application of substantive PBD principles to legacy data systems it is clear that such systems must be handled differently in some circumstances. When a company maintains legacy systems, it can be difficult to apply modern data handling techniques. In such cases, process and policy should primarily dictate the treatment of the system. Limiting access to such a system is one way that process can be used to enhance privacy under such circumstances. If data are needed from legacy systems, additional techniques can be applied to the data when or if it is transferred to another, more up-to-date system for use.

---

[10] The Fair Credit Reporting Act 3 § 15 U.S.C. § 1681a] (2004). www.ftc.gov/os/statutes/031224fcra.pdf.
[11] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 48.
[12] http://privacy.yahoo.com/aim.

2.5 Marketplace Participation

The Commission asked how to incentivize the full range of stakeholders to develop and deploy privacy enhancing technologies. One way to encourage such behavior is to favorably call out the best practices of industry leaders. Many technologies – such as Yahoo!'s Ad Interest Manager – require significant engineering effort and planning to deploy, maintain, and enhance over time. While we did this with the goal of giving users unprecedented transparency into information used in interest-based advertising, public notice of exemplary practice is always appreciated and creates incentives for many businesses to reflect best practices in their own privacy design work.

Another incentive to deploy privacy enhancing technologies occurs when companies choose to partner only with other industry participants who will adhere to industry standards. Companies will want to adhere to industry standards when their prospective partners adhere to such practices and therefore will encourage them to do so too. Industry support and participation of companies committed to privacy enhancing technologies has increased significantly in just the past year (membership at the NAI has tripled and an estimated 95% plus of ads served in the US are now conveyed through an NAI member company).

In addition, consumer-facing signals (such as seals, icons, or lists of participating companies) can be important factors in building consumer trust – and industry participants have significant marketplace interest in ensuring a trustworthy marketplace.

3. Simplified Choice.

Yahoo! agrees that simple choice is absolutely essential for consumers. That is why, in 2008, Yahoo! re-designed its Privacy Center to further improve navigation, provide more information on special topics, and give special prominence to its opt-out page so users can easily find and exercise their choice to decline interest-based advertising, also known as online behavioral advertising, or OBA.[13]

In 2009, Yahoo! provided logged-in users with tools to make their choice to opt out of OBA persistent.[14] It also added a new footer link called "About Our Ads" (in addition to our "Privacy Policy" link) to almost every page on Yahoo.com so that more information about its ad personalization and serving practices became "just a click away." In collaboration with others in the industry, Yahoo! launched experiments in new forms of user notice in close proximity to

[13] http://info.yahoo.com/privacy/us/yahoo/details.html is available from nearly every page of yahoo.com. The privacy policy allows users to look at products, topics, preferences and general help in addition to the core policy on the privacy home page. The easy to navigate structure allows users to get what they want quickly and intuitively.

[14] Users who elect to do so can associate their opt-out with their Yahoo! account – this means the opt-out will be refreshed each time a user logs in on any computer or device.

ads.[15] Yahoo! has also served over two billion public service announcement ads explaining ad personalization and serving practices. In Yahoo!-specific public service announcements (as opposed to ads on behalf of the wider industry efforts) a link to user controls for interest based advertising was included. Finally, Yahoo! launched Ad Interest Manager in December 2009, as mentioned above. Yahoo! makes AIM available through its privacy policy (which is accessible from nearly every page of yahoo.com) through public service ads about interest-based advertising displayed on our website, and through links from labels placed in or around advertising on our website. Yahoo! has been moving toward labeling ads that appear on our website since mid-2010 as part of larger industry self-regulation through the Digital Advertising Alliance known as the Advertising Option Program, and to date has displayed the icon over 1.3 trillion times.[16]

As a further simplification for users, multiple participants in the ecosystem are represented in one user interface from the label on an advertisement. Options to proceed to industry-wide controls such as those provided by the Network Advertising Initiative for ad networks, or the Digital Advertising Alliance work on the Advertising Option Program for a broader cross-section of participants in the OBA ecosystem, are easily accessible. Yahoo! is also experimenting with a possible next iteration of ad labeling notices, found by clicking on the ad label that appears above the ad on http://green.yahoo.com/living-green. In this iteration, additional industry participants involved in the ad serving event could also be highlighted, as could controls they offer. We believe this amounts to a "nutritional label" approach for OBA based on the metadata sent along with the advertisement, which could be further developed in the future.

3.1 Commonly Accepted Practices

Commonly accepted practices are essential to the basic functionality of the Internet, because websites need to collect data in the normal course of business for numerous reasons such as fraud detection, security defense, billing, determining which parts of a website are or are not being used, rendering a page in a format appropriate to the device and in the appropriate language, retrieving content data and displaying ads. The FTC framework appears to recognize this reality.[17]

However, it is hard to know what will be commonly accepted in the future, or when a practice moves from one category to the next. Amazon.com introduced a

[15] In 2010 Yahoo! joined in implementing an industry standard for use of the "power i" icon which can be seen on ads on the front page of www.yahoo.com and on many ads throughout the site as well as a transition to the "forward i" icon when possible trademark concerns were raised with the "power i".

[16] See http://www.clickz.com/clickz/news/2015791/dma-enforces-icon-rules-expose-violators. January 31, 2011.

[17] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 53.

recommendation engine over a decade ago to some strong concerns. However, most would say this practice is commonly accepted today, and has been for years.

What factors led to such acceptance? Was it simply experiencing the utility? Was it a period of time over which no particular harm was documented? Yahoo! suggests there are core values– for example utility or the overall value exchange – that make a practice commonly accepted over time. Recognition that accepted practices will change over time must be built into the overall framework.

3.1.1 First Party Marketing

First party marketing where data are used for the benefit of website users (or consumers/customers offline) and for the improvement of its services should always be considered commonly accepted practice. Website users likely intuitively understand that a website has access to the data generated while they are on the site. Users should also appreciate that, like in the offline world, data can be compiled from various sources to "better understand" customers. Where data are readily available, it should be understood that a company may obtain it – often for aggregation into marketing groups. For example, Yahoo! has obtained improved address information for some of our registered users to better match up with offline marketer designated market areas, or DMAs. The addition of this data does not convert data that is not personally identifiable to a state where it is; rather it facilitates marketing purposes and brings parity with marketing practices in the offline space. Such appends are reasonable practices that benefit users by bringing them more relevant and local opportunities and should be considered commonly accepted.

In addition, data may be used to reach an online company's customers via communication methods other than the Internet. There is no reason why an online company should not be treated in the same manner as an offline retailer that is able to contact its customers through email or postal mail. Limitations on the customer relationship in this way would significantly disadvantage online companies vis-à-vis their offline competitors. Of course, these communications should be subject to relevant laws such as CAN-SPAM.

3.1.2 Service Providers

The Commission appears to preclude any third parties collecting data directly (as opposed to having the data transferred by the first party) from being considered service providers subject to Commonly Accepted Practices. In the offline world, one can easily imagine a service provider operating the security cameras for a retail store. The video footage collected directly by the service provider is very

likely restricted to use on behalf of the retail client – or perhaps to improve the overall security services of the service provider such as for training new employees. This permissible offline concept should be equally applied online, including in the advertising space. For example, if a company is collecting data to provide a service such as analytics to a first party website and is restricted from using the data on behalf of other clients (but perhaps has permission from the first party site to use the data to improve its overall analytics algorithms), the use of the data for such improvement purposes should not negate its standing as a service provider, placing such activity in the Commonly Accepted Practices category.[18]

3.1.3 Commonly Branded Affiliates as First Parties

Marketing by commonly branded affiliates should be considered first-party marketing since there is little chance of consumer confusion. Today, Yahoo! maintains certain brands that include acquired companies, but that are generally also branded with Yahoo!, such as "Flickr, a Yahoo! Company", or "Right Media, a Yahoo! Company". And, while we maintain data that can be reasonably transferred among commonly branded affiliates, we choose to maintain "data firewalls" in some cases. For example with Right Media, Yahoo! must participate on the Right Media advertising exchange in the same way as any other exchange members – with no advantages through shared data. This restraint is dictated by the nature of the exchange rather than through ownership.

3.1.4 Sensitive Data

Sensitive data remains an ill-defined term, and the threshold for such a definition is difficult to determine. However, Yahoo!'s approach to the issue is twofold. First, Yahoo! assesses whether the creation of certain interest-based marketing categories is appropriate. For instance, Yahoo! does not create interest categories about sexual orientation or sensitive health information such as cancer for advertising customization. We also do not create categories specifically intended to target children under the age of 13 or use information from children we know to be under 13 to serve interest-based ads. Second, through our AIM product, a consumer can opt out of categories related to topics they wish to turn off. And, if they would like to opt out of interest-based marketing altogether, they are given

---

[18] Data Analytics has long been considered a standard practice in the online advertising industry. NAI guidelines have recognized this fact throughout its codes of practice, treating these practices quite differently from Online Behavioral Advertising. *Network Advertising Initiative. 2008 NAI Principles: The Network Advertising Initiative's Self-regulatory Code of Conduct. Network Advertising Initiative, 2008. NetworkAdvertising.org. <http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf>. Page 4.*

that choice as well. Additionally, Yahoo! provides a full list of our standard interest-based categories for user review. By using this approach, Yahoo! has been able to address the sensitive data issue by dealing proactively with the most commonly accepted "sensitive" categories for exclusion and allowing customers with additional privacy and relevancy concerns to address their choices directly. As with definitions of "appropriateness" across many different kinds of media, the breadth of sensitivity categories will depend upon many user variables and any attempt to legislate or regulate the meaning of "sensitive data" will end up being over-inclusive for some and under-inclusive for others at the same time.

3.2 Informed and Meaningful Consent

Yahoo! strongly agrees that context is essential to informed and meaningful consent in many circumstances. The *informed* nature of consent is the characteristic that is most dependent on context. Traditional interpretations of this element of consent have tended to place primary importance on the temporal aspect of consent (that is, the point in time when the user "signifies" their agreement), at the expense of other, crucially important contextual factors such as indicators of the presence of, or transfer of data to, third parties.

The Commission correctly points to context as being perhaps more important than the type of consent (opt-in v. opt-out).[19] It is unfortunate that there has been such a polarised debate between those in favor of "opt-in" approaches to consent and control (broadly defined as ruling something out unless a user has expressly chosen to accept it) and those in favor of "opt-out" (broadly defined as a situation where the user is allowed to stop something that would otherwise proceed). "Opt-in" has come to be perceived as more protective of users' privacy than "opt-out". The result has been a drive by privacy advocates (and indeed by many legislators) to push for "opt-in" approaches to data protection as the norm. In recent years, however, it has become evident that a poorly-designed "opt-in" (for example, one provided out of context) is less protective of privacy than a well-designed, well-timed "opt-out".

Two examples of informed and meaningful consent in context are the Digital Advertising Alliance Advertising Icon Project referred to earlier, and the launch of Yahoo! Updates in 2010.[20] The transparency and control provided by the icon are immeasurably enhanced by its proximity to the ad. Consumers should intuitively understand that it is related to advertising and may take action at the time and place their data are being collected or used.

---

[19] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 60.

[20] The DAA project is more fully explained at http://www.aboutads.info/

When Yahoo! launched Yahoo! Updates last year, it provided contextual controls to users before they published information via "status updates" or "like buttons". Users have the choice to publish these actions to "everyone"(public) or "connections"(friends) on the Yahoo! network, or to publish to Facebook, and now Twitter. In addition they are reminded of the way the message will appear to others, its breadth of sharing and are separately offered an opportunity to change their picture or avatar and to change the name that will appear with the message through additional settings. This is a contextual way to remind users that they have control over settings – provided at the time of publication in the context of the action they are taking. Yahoo! believes this is the most appropriate approach to informed and meaningful consent in areas where users are posting content.

3.2.1 Mobile considerations

Industry has strong incentives to continue to innovate and develop workable solutions for the nascent, burgeoning mobile sector to ensure mobile users are comfortable engaging with mobile commerce and applications. Initial thinking about mobile privacy began with analysis of how the fair information practice of "notice" could transfer from personal computers, or PCs, to mobile devices in a meaningful way, but has departed from the premise that PC-based privacy practices need to be adapted to fit smaller screens. Yahoo!'s experience in this area reveals more distinctions between the online PC-based and mobile environment than many commonly acknowledge in policy discussions to date. This discussion requires a deeper consideration and analysis of the complexities of the mobile ecosystem than mere "screen size."

Unlike the rough standardization in the online PC-based sector thanks to relative consolidation around a small number of browser interfaces, there are a plethora of diverse interfaces presented by mobile device operating systems, application layers, and carriers. The functionality, diverse operating systems (users interact with multiple OS versions varying in their approaches to privacy), browsers and applications developed for these interfaces can vary significantly from device to device. This makes it extraordinarily difficult for companies to develop "one size fits all" approaches to notice or indeed to privacy across multiple platforms and services. Moreover, industry participants with different roles in the mobile ecosystem — device manufacturers, operating system providers, application providers, carriers, OEMs, etc. – may assume different roles as they take on the responsibility with respect to user privacy. Individual companies may also concurrently operate in several of these roles.[21] Although the Commission

[21] For example, Apple and RIM are operating system providers, browser developers, application developers and distributors, content publishers and device manufacturers. Google is an operating system provider, a browser

recognizes the diversity of the mobile ecosystem when it states "All companies involved in information collection and sharing on mobile devices – carriers, operating system vendors, applications, and advertisers – should provide meaningful choice mechanisms for consumers," Yahoo! believes that the Commission overstates the ability of some ecosystem participants to provide those mechanisms. [22]

Yahoo! has experienced the very real challenges of providing notice in non-personal computer environments such as in smartphones and tablets. In some cases, such as when an operating system controls the geo-location acquisition permissioning for a device, the operating system may restrict Yahoo!'s ability to directly provide choice to the user and also limit Yahoo!'s ability to even understand which choice the user made. Accordingly, there are circumstances in which the user is solely subject to the privacy settings disclosed and managed by the operating system. However, where Yahoo! controls notice flows to our users, we generally offer simplified notice on the device, layered with more comprehensive notice available from the main privacy policy. Yahoo! also supports its users by prioritizing online access to mobile-specific privacy information so that, notwithstanding any device-specific constrains or limitations, users can readily access policies and controls via any web-connected device.

Devices with limited user interface options, such as in the mobile environment, will receive more scrutiny from industry in the coming months. Industry associations and mobile systems experts are consolidating in trade bodies to determine how privacy can be applied both flexibly and meaningfully by the respective participants, alone or in collaboration, that make up this complex ecosystem. Yahoo! will continue to collaborate and learn from these efforts.

3.2.2 Durable Opt-out

A key component of informed and meaningful choice is a durable opt-out. As previously mentioned, Yahoo! made many improvements to its interest-based advertising opt-out in 2009. Yahoo! extended the opt-out to its mobile platform – including persistence for logged in users. This allows user choice to seamlessly flow across computing devices through logged-in experiences. It changed opt-out cookie expiration dates from the standard two years applied to Yahoo! cookies to 20 years so that opt-out cookies are less likely to expire – making user preferences

---

developer, an application distributor, a content publisher, and an application provider. Verizon and AT&T are both applications providers, content publishers, and carriers.

[22] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 59.

more durable. Yahoo! also updated its web servers and data handling processes to remove opted-out user activity from our ad interest systems Finally, we've extended the concept of a durable opt-out to our advertising exchange business, Right Media, where we support our customers efforts in respecting consumer choice by enabling them to effectuate their own users opt-outs on the exchange.

3.2.3 Take it or Leave it

The report requests input on whether and under what circumstances choice could be offered as a "take it or leave it" option, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices. Since the inception of the commercialized internet, users and website providers have understood that website terms of service and privacy policies constitute binding agreements between them. That framework has become fundamental to use of the web, with disclosures of site terms and data use online far exceeding similar disclosures in many offline situations. Yahoo!, for example, serves up its TOS for user review and consent during site registration and also calls out critical information in specialized links within the footer of most of its site pages, including a link to its privacy policy, information "About Our Ads", Safety, the Terms of Service and Copyright/IP policy. It is true that site terms of service are binding but because websites compete to offer more value to their users, if users do not see such value or if they object to website terms of use, they go elsewhere. Users have choices and because of vibrant competition on the web, they can freely exercise those choices.

One additional point about website terms of services deserves special mention. Today, many sites, including Yahoo!, let consumers access portions of their sites and services, subject to their Terms of Service, without having to register or to create an account. If the Commission's guidance in this area implies that such an arrangement is invalid or lacks force of law, then website operators will likely protect themselves by requiring users to pre-register in all circumstances and consumers will be compelled to provide more personal information to sites than they often do today. This seems to be a perverse and unintended result.

3.3 Enhanced consent for sensitive information

The Commission calls out sensitive information as an area where it recommends affirmative express consent be employed. As discussed earlier, the first obstacle with such an approach is the difficulty in defining categories of sensitive data and the fact that "sensitive" is a term defined differently by different people. Yahoo! believes that the focus should be on the quality and content of the notice and consents in general, making the distinction between sensitive and non-sensitive data less relevant.

Even if the Commission does try to define "sensitive", the paper raises a new concept. In the Commission's discussion of consent for sensitive data in previous papers, enhanced consent would apply to collection *and* use of the information, and primarily in the OBA context.[23] In this report, the Commission has applied enhanced consent for collection *or* use *or* sharing, which indicates that simple collection of information is of concern, even if it is not used or shared.[24]

This goes well beyond the previous context of OBA implicating information users may generate on their own, such as search terms or status updates. Certainly, search terms in the area of health should not be treated with the same level of sensitivity as medical diagnoses. In the area of finance, the creation by a user of a stock tracker should not be treated in the same way as financial account information. In general, marketing data simply does not rise to the level of "sensitive". And collection of such data should not trigger enhanced consent.

In terms of gaining affirmative consent when a user chooses to disclose sensitive information, Yahoo! believes affirmative consent is given when an action to publish is taken by a user. A website is not able to control what data are posted by a user, and an opt-in consent beyond that which is implied by the publishing act itself every time a user posts "just in case" seems overly intrusive and irrelevant in most instances.

3.4 Information brokers and meaningful choice

The Commission points out that certain entities such as information brokers do not have direct relationships or interactions with consumers. In such cases, information brokers should maintain a public facing website where consumers can interact with the information broker, and companies using their services should disclose that fact in their privacy policies with appropriate links back to the information broker's web presence.

Yahoo! is a leader in industry by disclosing advertising third parties we work with contractually in our privacy policy.[25] We believe this should be a more standard practice. Where we act as a third party ad server on other publishers' sites, we contractually require that there be a link to either Yahoo!'s opt-out or the NAI industry-wide opt-out from their privacy policies or enhanced contextual notices so that consumers have fairly easy access to control features. The Digital Advertising Alliance industry code adopted

---

[23] The Federal Trade Commission Staff. Self-Regulatory Principles For Online Behavioral Advertising. Rep. FTC, Feb. 2009. <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.Page 43-44, 47.

[24] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 61.

[25] http://info.yahoo.com/privacy/us/yahoo/thirdparties/details.html

by the Direct Marketing Association requires entities collecting or using data for OBA to disclose that fact outside of the publisher's privacy policy – this is done through links such as "About Our Ads" or through the Advertising Icon Option referenced earlier. Further, many data brokers have banded together in a program to provide transparency and accuracy for data brokers.[26]

3.5 Do Not Track

Yahoo! values the Commission's statement that "any such mechanism should not undermine the benefits that online behavioral advertising has to offer, by funding online content and services and providing personalized advertisements that many consumers value."[27] This statement is of critical importance.

In Yahoo!'s experience, although users understand the need for data collection for the provision of innovative services, they want to understand more about its use – the "why" their data are being collected and "how" it will be used and possibly re-used. A move away from a focus on data collection is advocated in the recent Commerce Department Green Paper, which allows industry to direct attention to providing easy-to-use privacy tools while allowing data-dependent operation of the Internet to proceed, to the benefit of users.[28] Yahoo! believes this is the only workable direction for regulation.

Those Do Not Track (DNT) proposals that eliminate basic data collection do not allow for routine Internet operations, and should therefore be rejected as impractical and highly disruptive of consumers' online experiences. The Commerce Department has acknowledged that certain approaches to DNT could have harmful effects on the Internet – which would clearly be the case for a collection-based approach.[29] In addition, such a DNT framework does not account for the nuance or level of choice many users may want, such as a user who prefers personalized services, but not online behavioral advertising.

Radically simplified choice for consumers is the goal of DNT proposals, and informed choice is a goal with which Yahoo! agrees, even though we see significant flaws in some approaches to the DNT model. The FTC has recognized DNT cannot operate under a

---

[26] A recent effort by Evidon™ enables advertisers and other businesses to give consumers the ability to opt out of further targeting. *See more at* http://www.evidon.com/consumers/engage.

[27] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 67

[28] "*Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*" The U.S. Department of Commerce. Internet Policy Task Force. 16 Dec. 2010. <http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf>. Page 33.

[29] Danny Weitzner, Associate Administrator for Policy, National Telecommunication and Information Administration, U.S. Department of Commerce. *"Testimony before the Energy and Commerce Committee of the U.S. House of Representatives".* 2 Dec. 2010. http://www.ntia.doc.gov/presentations/2010/ConsumerWatchdogPolicyConference_12012010.html

registry model, as does the Do Not Call Registry.[30] This is primarily because unlike the phone numbers used by the Do Not Call Registry, no single, consistent identifier is used by every online service to facilitate online interactions.

Many identifiers used today on the Internet, such as company-specific cookies, "remember" settings and information about a user or device. Unlike a phone number, a cookie can easily be deleted. It is common for browsers to allow users to adjust settings so that certain cookies or all cookies will not be set, or will be eliminated after the specific browser session, and some security products routinely eliminate certain cookies from machines where they have been installed. In addition, it is common practice for industry participants to allow users to "opt out" of having data remembered in cookies for the purposes of OBA. This means there are numerous ways in which consumers are protected from unwanted state maintenance or tracking.

Some proposed DNT approaches would require all websites be reengineered in order to read header data that could be broadcast by browsers. If this approach is focused on third party "servers" and broadened to encompass all data collection, even the basic rendering of content, would be disrupted, as the server would not receive instructions from the browser to send the requested content. This "breaks" many websites, including Yahoo!, that aggregate or license content from third parties– or support and supply content for third party sites. The Internet is currently at a stage where the presence of third parties is commonplace on most websites, and is both accepted and even desired (for instance, the aggregation of news articles, photographs, and user generated content from multiple sources across the Internet). Yahoo! brings together the best content of the web. At times we create our own content, we license content from others in many cases, and in still other cases we create platforms where contributors can easily post content. An examination of our site will reveal many third parties present for content as well as ad serving. Thus, such a proposed browser broadcasting approach would be a very disruptive experience for users and should not be considered when other less disruptive tools are at hand.

In fact, Yahoo! has participated in the Advertising Options Program in part because it is an easy, one-stop shop for controlling OBA, while allowing the entity displaying the ad to offer users more granular choices related to its advertising (such as AIM). Some proposed browser tools take fairly blunt "one size fits all" approaches by blocking third party URLs or broadcasting a signal to all third parties that they should not collect or return data. These approaches are not only disruptive, they do not allow users the level of

[30] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 63.

choice Yahoo! has worked hard to provide in AIM, and thus provide *fewer* meaningful choices to consumers. The Commission has noted that many users appreciate this additional level of choice, but it is difficult to see how it would be provided in browser-based approaches, unless the browser providers were to develop standard industry interest categories.[31] Yahoo! objects to such an approach because it does not allow companies to create the most appropriate characterizations of interest for their customers. Further, Yahoo! objects to making browsers the arbiters of online advertising segmentation, especially given that many popular browsers are developed by Yahoo!'s competitors in the ad serving business, such as Microsoft and Google, and likely will not be implemented in a disinterested manner.

The DAA Advertising Option Icon approach is the strongest DNT proposal available, and the most in line with the caution not to undermine the benefits of OBA outlined by the Commission. While it is not a full solution for those who want to stop *all* collection of data (again, there are key reasons why much routine data collection needs to occur as referenced above) it covers the largest swath of technologies used to remember user activity in the marketplace today, and is growing in size and scope.[32] The proximity of ad labels for this option make the accessibility of information about ads and links to opt-outs that cover most of the advertising industry unprecedented and hard to miss. As the program continues to roll out, additional educational efforts will help users better understand the meaning of the symbols they see in or around ads. Yahoo! will be doing its part; as mentioned above, Yahoo! has displayed the icon over 1.3 trillion times. Yahoo! believes this effort is a strong answer to calls for DNT through enforceable self-regulation and should be further encouraged by the Commission.

4. Increased Transparency

Yahoo! supports increased transparency for users as evidenced by the introduction of the numerous privacy features in our privacy policy and represented by AIM. The Commission contemplates a framework where users are notified of important information outside of privacy policies, and industry is certainly moving in that direction in the area of OBA. However, privacy policies continue to provide extremely important functions, including serving as the document against which the FTC can base claims of unfair and deceptive practice should a company not follow the policy. The means of collection and the uses of data are as diverse as the companies represented in our economy. Therefore, the belief that a single comparison framework could be

---

[31] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 67-68.

[32] See the Digital Advertising Alliance website page on Member resources and services (http://www.aboutads.info/participants/). See Evidon Company Database, which includes every business that uses audience data in some way, including for online behavioral advertising (http://www.evidon.com/consumers/profile_manager).

developed for such varied businesses, that is applicable both online and offline, is difficult to conceptualize.

One method discussed by the Commission is machine-readable policies. This holds great promise for the future. Some methods have been tried in the past, such as the P3P approaches of the late 1990s. Yahoo! participated in that effort, (and supports P3P even today across all Yahoo.com cookies) but it did not gain broad, industry-wide acceptance. The DAA Advertising Option Icon program is moving towards including "metadata" that is sent with advertisements. In the future, this metadata can be used to bring additional transparency for all companies involved in the serving of an online ad – including third parties such as data brokers.[33] The technology industry continues to innovate in the area of privacy, and it is likely that we will see more innovation on this front if these approaches are supported by the Commission.

3.1 Access to Consumer Data

Yahoo! strongly agrees with the Commission's determination that "companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and nature of its use."[34] Yahoo! provides transparency through AIM, and we've previously discussed reasonable access in section 2.3. We understand that reputable data brokers are providing consumers access to much of their data (anti-fraud databases being a notable and reasonable exception). The most important factor for access is "reasonableness". Yahoo! designed AIM not to show users every log entry or click on the website, but rather to present standard categories and general areas of activity to help them understand what is used to target advertising. Consumers could not process or be expected to understand every data point, or to read lines of code.

A sliding scale may be an appropriate framework for determining access as well. Data used for a purpose covered by the FCRA already has access and notification procedures around it. As previously stated, Yahoo! does not believe marketing data rises to the level of "sensitive" data, and is unlikely to be used to "deny benefits". If such data are used to deny critical benefits such as employment, credit or insurance, then FCRA applies and no new rules are needed. Therefore, solutions like AIM fit comfortably within a sliding scale approach. In addition, recognition of cost versus benefit in individual cases is a significant factor called out under the framework. [35] As a clear rule, any framework for

---

[33] Again, see Yahoo!'s next generation implementation at http://green.yahoo.com/living-green

[34] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 72.

[35] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." The Federal Trade Commission, 1 Dec. 2010. <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>. Page 74.

access should not require companies to treat anonymous or de-identified data as personally identifiable.

Finally, with respect to teens, Yahoo! allows parents to have overall control of a child's account through Family Accounts. A parent may change settings and access to various Yahoo! products and services, and can eliminate a child's account at any time.

4.2 Consumer Education

Consumer Education is a critical component of building online trust. Yahoo! seeks to educate its users through ad labeling, public service announcement ads on interest-based advertising, the "About Our Ads" link and the privacy policy – in particular the "topics" tab.[36] As previously mentioned, Yahoo! has shown over two billion PSA ad impressions, and over 1.3 trillion icon impressions to date. These education efforts are important and will continue.

The Commission's role in education is also quite important – especially among groups more likely to trust government information than industry information. The work of OnGuard Online has played a critical role in educating the public and providing information for dissemination through educational institutions.

Again, thank you for the opportunity to comment on these critical issues. Yahoo! looks forward to continued discussions with the Commission as it forms its final framework recommendations in the months ahead.

Respectfully submitted,

Anne Toth

Chief Trust Officer

Yahoo! Inc.

[36] http://info.yahoo.com/privacy/us/yahoo/topics.html