



Via Email: privacynoi2010@ntia.doc.gov

Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

RE: Comments on “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework”

Dear Internet Policy Task Force,

Thank you for the opportunity to comment on the recently released Green Paper issued by the Internet Policy Task Force entitled “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework”. The Green Paper marks the new beginning of an important dialogue between the Administration and various stakeholders on the future of global Internet privacy. Indeed, the Green Paper recognizes that addressing these important issues requires “reinvigorating the commitment to providing consumers with effective transparency into data practices, and outlines a process for translating transparency into consumer choices through a voluntary, multi-stakeholder process,” and is precisely the type of cooperative effort we believe will garner the best results for consumers and industry alike.¹

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.

Founded in 1994 by Stanford Ph.D. students David Filo and Jerry Yang, Yahoo! began as a hobby and has evolved into a leading global brand that changed the way people communicate

¹ “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 iii

with each other, conduct transactions and access, share, and create information. Today, our U.S. flagship property Yahoo.com, operated by Yahoo! Inc., attracts hundreds of millions of users every month through its innovative technology and engaging content and services, making it one of the most trafficked Internet destinations and a world class online media company. From the global perspective, our offerings to users on diverse Yahoo! Properties currently fall into five categories: Integrated Consumer Experiences, Applications (Communications and Communities), Search, Media Products & Solutions, and Mobile. The majority of our offerings are available in more than 30 languages. The company is headquartered in Sunnyvale, California, with a presence in more than 25 countries, provinces, and territories.

Yahoo! is pleased to see the creative approaches to policymaking represented in the Green Paper. We hope the U.S. will take a strong leadership role as countries around the world begin to address these important issues. We commend the focus on maintaining innovation and growth of the Information Economy that has flourished under the current U.S. approach, while exploring meaningful frameworks to address new marketplace developments with respect to commercial data. To advance in step with the marketplace itself, governing in the Internet era must equally value privacy and innovation as important policy goals. The Green Paper 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 We urge the U.S. to remain committed to this dual emphasis as it develops bilateral or multilateral frameworks for treatment of user data with its global partners.

It is no coincidence that the U.S. is the birthplace of most of the widely used global websites and online services. Our 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 Green Paper below.

1. Baseline Commercial Data Privacy Framework and Fair Information Practice Principles (FIPPs).

Over the last decade, the adoption and implementation of fair information practices principles has helped consumer trust and use of the Internet grow and flourish while enabling unparalleled innovation. Continuation of this FIPPs-based approach will yield concrete movement toward a harmonized global privacy framework and will support flexible privacy protections that support both innovation and consumer needs. FIPPs is a common language used by many governments

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

worldwide, so use of similar terminology will enhance opportunities for agreement and practical approaches to data policy. However, within a FIPPs framework there are some important considerations to note.

1.1 Recognizing that Not All Data is the Same

For a FIPPs framework to succeed, all parties must speak the same language when defining the data covered by privacy frameworks. Historically, U.S. privacy laws have regulated use of “personally identifiable information”, or PII.³ Privacy policies and internal procedures were predicated on reviewing the use of data sets that specifically identified users in areas such as name, address, social security number and the like. In recent years, with the emergence of practices such as Online Behavioral Advertising, or OBA, and other practices which may result in logging the interests of users across websites and over time, some have suggested the PII definition is insufficient to address the needs of users. However, in considering alternative approaches, simply expanding FIPPs treatment to all technical identifiers in the same way that PII has been treated would be overbroad and inflexible in addressing both the privacy needs of users and commercial interests.

FIPPs were developed and embraced in the U.S. in a setting where PII was the primary concern. Accordingly, certain FIPPs may not apply to non-personally identifiable data in the same way or with the same urgency as PII.⁴ This must be acknowledged in any implementation of FIPPs. Moreover, a significant qualitative difference between PII and non-PII cannot be overlooked. Cookie identifiers used in OBA are not universal identifiers that can be interpreted by all, nor do they contain personally identifiable information in most cases. In fact, OBA systems primarily rely upon use of cookies *because* cookies allow recognition without the use of personally identifiable information. Even without regulation, Yahoo! has been a leader in creating tools to manage privacy in new environments like OBA through Ad Interest Manager and CLEAR Ad notice (discussed in Sec. 2.1), which enable users to understand and to control their online experiences even with cookie-based data elements not traditionally covered under U.S. privacy frameworks. Reasonable applications of FIPPs are likely to mirror these marketplace developments.

³ Indeed, the Department of Homeland Security FIPPs included as an example in the Green Paper specifically apply to PII. “*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 26.

⁴ For example, under an access FIPP, consumers may have no desire to see (or derive much value from seeing) every log entry a company has on them (resulting from an expanded scope to apply the standard to any identifier). The same consumers may have a greater interest in seeing data if it leads to an adverse action covered by the Fair Credit Reporting Act, such as a credit score.

1.2 Enforcement based approaches – ex post regulation has driven innovation and growth

The enforcement-based approach to commercial data taken in the U.S., sometimes referred to as an ex-post approach in international circles, has yielded much progress in both innovation and in privacy-protective tools for users. This approach relies on the FTC to use its broad enforcement authority under Section 5 of the Federal Trade Commission Act dealing with unfair or deceptive practices, and also on non-governmental organizations, or NGOs, to hold entities to codes of conduct. NGOs serving as compliance bodies for such codes enforce the codes against their members and can escalate concerns to regulators or publicly cite or throw out members not adhering to the codes. NGOs that do not serve as compliance bodies, but watch out for consumer concerns nonetheless, can also bring apparent violations to regulators' attention. Comments by Jacob Kohnstamm, Chairman of the Dutch Data Protection Authority and Chairman of the EU Article 29 Data Protection Working Party, and Neelie Kroes, Vice President of the European Commission and European Digital Agenda Commissioner, indicate that other countries are exploring and moving toward ex-post approaches to privacy regulation as they look for practical ways to enhance privacy compliance and enforcement without creating undue process burdens, also noted as a goal in the Green Paper.⁵ Questions raised in the Green Paper about possible legislation, which would constitute ex-ante rules, are valid and important, but for the reasons set forth in succeeding sections of this comment, the ex-post approach should not be abandoned; rather, it should be further embraced and touted to other global regulators.

1.3 FIPPs will Work Best with Flexible Implementation

One reason why a FIPPs-based approach has been successful in the U.S. is that it can be implemented flexibly, largely through voluntary self-regulatory efforts, enhanced by government enforcement. As innovation continues apace, inflexible rules that often come with government regulation can unintentionally stifle marketplace developments that make users' Internet experiences richer and more satisfying. As the Green Paper states, a multi-stakeholder approach will garner the best results. FIPPs can be most effectively implemented through voluntary self-regulation approaches that rapidly and flexibly adapt to changes in the marketplace. By contrast, legislation and its regulatory implementation are almost always time consuming, producing policy outcomes that are frequently

⁵ “*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 31; See remarks of Jacob Kohnstamm “*Creating a Modern and Harmonized Regulatory Framework*” at European Data Protection and Privacy Conference, 30 November, 2010. Neelie Kroes Remarks at the European Roundtable on the Benefits of Online Advertising for Consumers, 17 September, 2010.

outpaced by marketplace developments. Further, broad-based self-regulation with built-in enforcement regimes can be effectively enforced by the Federal Trade Commission under existing statutory authority, as well as by non-governmental organizations.⁶ Given the proven consumer benefits produced under the last decade of innovative self-regulatory initiatives coupled with government oversight and enforcement, this model can and should remain the centerpiece of the U.S. approach.⁷

2. Enhanced Transparency Should Be A Key Goal

As the Green Paper states, the ultimate goal of a FIPPs-based approach should be greater substantive privacy protection for consumers. As also noted, transparency in collection and data use policies is critical to achieve that goal. Yahoo! believes that enhanced transparency can be achieved through multiple methods. For instance, within privacy policies, a layered notice approach can get people to information they seek more quickly and more easily. A modern approach to transparency also calls for contextual notices where appropriate, such as in conjunction with OBA and when users post content.⁸ Notices can explain new features or functionality. Finally, ongoing educational efforts such as videos and privacy or safety-focused public service announcements can be used to enhance transparency. As described below, the evolution of Yahoo!'s approach to transparency offers a clear example of the benefits of the integration of policy, technology and presentation in enhancing user privacy.

2.1 Technology should play a strong role in bringing greater transparency to privacy policies

Various entities have created technology tools to enhance privacy through additional transparency. Yahoo! recognized early in its history that users should understand what information it collects, how the information is collected and used, and – just as importantly – how Yahoo! must work to manage and protect such information. In 1998, Yahoo.com became one of the first sites in the United States to develop and publish a

⁶ The Network Advertising Initiative and the Direct Marketing Association each have enforcement mechanisms bolstering FTC efforts. See <http://www.networkadvertising.org/managing/enforcement.asp> and <http://www.the-dma.org/index.php>.

⁷ "The IAB Europe/McKinsey study shows that advertising triples the value consumers receive from the Internet, by subsidizing such valuable services as email, comparison shopping, news alerts, social networking, and video entertainment," said Randall Rothenberg, President and CEO, IAB US. "Consumers Driving the Digital Uptake: The Economic Value of Online Advertising-based Services for Consumers." IAB Europe, Sept. 2010. <http://www.iab.net/media/file/White-Paper-Consumers-driving-the-digital-uptake_FINAL.PDF>

⁸ Yahoo! continues to implement ad labeling throughout yahoo.com as part of the Digital Advertising Alliance efforts including "Ad Choices" links from ads on yahoo.com and in most ads Yahoo! sends through our Ad Network. In addition, Yahoo! provides visual clues and tools allowing users to control where and to whom content they create will be displayed, such as on Yahoo! or also on Facebook or Twitter, and to contacts, everyone or no one.

comprehensive privacy policy, which could be found through a prominent link on its home page and in the footer of nearly every other page on the Yahoo! site. In 2002, Yahoo! again led the industry by introducing a layered “Privacy Center” model on top of its existing privacy policy. This model reflected Yahoo!’s rapid expansion into a wide array of online services, and it was designed to help users more readily find privacy-related information about the specific Yahoo! services that interest them – without requiring them to navigate information about services they did not use. In 2008, Yahoo! re-designed its Privacy Center to further improve navigation, provide more information on special topics, and to give special prominence to its opt-out page so users can easily find and exercise their choice to decline interest-based advertising.⁹

In 2009, Yahoo! provided logged-in users with tools to make their choice to opt-out of OBA persistent.¹⁰ It also added a new footer link called “About Our Ads” 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 ads.¹¹ Yahoo! has served over two billion public service announcement ads across the Web Site explaining ad personalization and serving practices. In the Yahoo! PSAs (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 (<http://privacy.yahoo.com/aim>) (AIM) in December 2009, which allows users to see what standard interest categories they are placed in for interest-based advertising purposes, as well as controls for modifying those categories or such advertising as a whole.¹² AIM also allows consumers to see the types of data that contribute to those categorizations. This level of transparency is unmatched in the marketplace.¹³ Yahoo! makes AIM available through its privacy policy (which is accessible from nearly every page of

⁹ <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.

¹⁰ 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. Other opt out improvements included: 1) extending the opt-out to our mobile platform – including persistence for logged in users. This allows user choice to seamlessly flow across computing devices; 2) changing opt-out cookie expiration dates from the standard two years we apply to Yahoo! cookies to 20 years so that opt-out cookies are less likely to expire – making user preferences more durable; and 3) updating our web servers and data handling processes to remove opted-out user activity from our ad interest systems.

¹¹ 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”.

¹² http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html

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 has displayed the icon over one trillion times.

In the ad labeling model, multiple players are represented in one user interface. 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 players 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 players 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.

2.2 Increasing use of devices with limited user interface options

Industry has strong incentives to continue to innovate and develop workable solutions for the 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 many 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.”

First, 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 devices and carriers. The functionality, diverse systems, 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 players with different roles in the mobile ecosystem —

¹³ Yahoo! is not the only company to take such an approach. Google and Microsoft each have similar tools. 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>.

device manufacturers, operating system providers, application providers, carriers, OEMs, etc. – may assume different roles as they take on the responsibility to respect user privacy. Individual companies may also concurrently operate in several of these roles.¹⁴ In addition, the industries supporting the mobile ecosystems are themselves evolving quite rapidly. The sector is undergoing a period of explosive and dynamic innovation and experimentation, which is changing monthly. The recent popularity in 2010 of tablet devices has changed much of the equation.

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 constraints 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 FIPPs can be applied both flexibly and meaningfully by the respective players, alone or in collaboration, that make up this complex ecosystem. Yahoo! will continue to collaborate and learn from these efforts.

2.3 The Efficacy of Privacy Impact Assessments Requires More Study

While PIA’s are undoubtedly useful in some circumstances, we do not believe that PIAs will be appropriate or cost-effective in all circumstances and that they may, in some cases, confuse consumers. Moreover, while we believe that privacy policies reflect a reasonable means of conveying privacy information, there is no reason to believe that consumers would access public postings of PIAs more frequently than they access

¹⁴ 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 developer, an application distributor, a content publisher, and an application provider. Verizon and AT&T are both applications providers, content publishers, and carriers.

existing privacy policies today. Yahoo! recommends that PIAs always be used on a voluntary basis.

A Move Away From Collection Focus is Critical

Yahoo! believes the Green Paper's acknowledgement that stressing collection and data minimization FIPPs is unhelpful when data collection is both prevalent and critical to bringing innovative services to market.¹⁵ At the same time, websites may need to collect data in the normal course of doing business for numerous reasons, such as fraud detection, 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 acknowledged this concept in its paper in a section on "Commonly Accepted Practices".¹⁶

In Yahoo!'s experience, although users understand the need for data collection for the provision of innovative services, they want to understand "why" their data is being collected and "how" it will be used and possibly re-used. A move away from a focus on data collection, as advocated in the Green Paper, directs industry attention to answering these important questions while allowing data-dependent operation of the Internet to proceed, to the benefit of users.

Discussions of Do Not Track, or DNT, proposals which 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 DOC has acknowledged that certain approaches to DNT could have harmful effects on the Internet – this would clearly be the case for a collection based approach.¹⁷ 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. (Further discussion of appropriate DNT approaches is in Section 3.3)

In contrast, a key strength of the purpose specification and use-based model lies in the increased likelihood that technological means can achieve meaningful privacy protection.

¹⁵ "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.

¹⁶ "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.

¹⁷ 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

Many Internet companies are structured so that they receive data centrally, but send it to many internal systems where the same data is used for many different purposes. Rather than limiting data collection at the outset, which obstructs basic operations, the focus on “turning off” certain systems and specific uses is a more practical solution. This implies that it may be better for policy discussions around data privacy to address specific harmful uses of information that can injure users, rather than on the limitation of data collection outright.

The use-based model also offers flexibility for innovation. For instance, controls on use have been designed around the posting of user-generated content allowing users to specify which uses are acceptable to them by engaging with tools offered by companies.¹⁸ Another example is the development of option menus around activities such as online behavioral advertising.¹⁹ Because use models allow companies to research and develop new uses for data and then to present them to users, this framework is highly compatible with the goal of encouraging innovation. Yahoo! recognizes that innovation around data use necessitates balanced pairing with responsible privacy practices.

Finally, where the Green Paper notes that purpose specification and use can create better alignment between practices and user expectations, it is helpful to consider that user expectations will rarely *anticipate* innovation. If everyone expected or anticipated it, a development likely wouldn't *be* innovative. Given industry's imperative to create more useful products and services in ways that are either respectful of privacy or privacy enhancing, discussion should continue around a path forward that recognizes the type and sensitivity of data at issue (PII or non-PII), the materiality of any change in use, and the relative benefits of any new uses to consumers. Privacy and innovation are compatible.

3. Self-Regulatory Frameworks

The most reliable and appropriate way to effectuate privacy enhancing change in the marketplace is through self-regulatory frameworks that are accountable and enforceable. Various elements of self-regulatory models are discussed below, followed by a discussion of enforcement issues, which are essential to the success of these frameworks.

¹⁸ See tools around Yahoo! Updates at <http://pulse.yahoo.com/y/settings/updates>. Tools around photos on flickr.com are available to manage not only who is able to see photos, but the licensing regime the poster chooses to place on the photo as well. As a result, this regime also works particularly well for copyrighted works generated by users.

¹⁹ <http://www.privacy.yahoo.com/aim>

3.1 Codes of Conduct

Yahoo! believes the creation of voluntary, enforceable industry codes of conduct will produce the specificity, dynamism and certainty desired by policymakers and industry alike. Such codes can more rapidly address emerging issues, more flexibly interpret certain FIPPs applied to specific situations, and more expansively engage both industry and civil society. This makes such codes an immensely practical approach to progress in commercial data policy. While the framework appears to emphasize the role of such codes for activities outside the scope of FIPPs, interpretations of FIPPs in new circumstances is a key role for such codes.

3.2 Development of the Privacy Policy Office with Convener Role

The Green Paper outlines the history of government involvement with privacy. Some of the most relevant discussion regarding commercial data policy centered on the role government can play as a convener. This is a particularly helpful role, especially where industry and civil society have talked past each other without agreement. It is critical that various stakeholders hear the views of others, and that practical solutions reflecting realities and user needs be developed. A broad swath of industry players and civil society will need to be represented for such an effort to be successful, as intended by the framework.²⁰ The Department of Commerce is well positioned to serve this role, and to export its success through international outreach.

A distinct benefit from the convener approach is the likelihood of more immediate success than a regulatory or legislative process. It does not follow though, that if industry and civil society cannot agree on voluntary codes of conduct that it should trigger an automatic move to rulemaking. The FTC has chosen not to exercise its current rulemaking authority in this area thus far, opting instead to give extensive guidance to industry. A dialogue where automatic rulemaking could be triggered actually creates perverse incentives for some entities to never reach agreement, which undercuts the intent behind “convening” the stakeholders.

²⁰ “The Dynamic Privacy Framework requires and authority to convene businesses and civil society to develop effective, consensus-based voluntary codes of conduct in a wide variety of commercial contexts. Identifying areas in which such codes are needed and bringing together the stakeholders will be critical to the Dynamic Privacy Frameworks’s success.”
“*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 44.

3.3 Do Not Track considerations

Another self-regulatory idea raised is Do Not Track, or DNT. 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 the DNT model. The FTC has recognized DNT cannot operate under a registry model, as does the Do Not Call Registry.²¹ 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. Moreover, 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 remembering or tracking.

Some DNT proposed approaches would require all websites to be reengineered in order to read header data that could be broadcast by browsers. Such an approach would likely also mean that any third party server, including those that would be rendering content, could not receive instructions from the browser to send the data. This “breaks” many websites, such as Yahoo! that aggregate or license content from third parties. 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! thrives as a site that 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.

²¹ "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.

As mentioned earlier, certain data is needed to facilitate the typical functionality of the Internet. Thus, “Do Not Track” is a misnomer if this basic functionality is to be preserved. Where the PPO may want to focus its attention is on uses of data that consumers want to control, such as OBA. The PPO can explore the best ways to simplify this process for consumers and can educate them on various approaches designed to give them control. Again, this more closely comports with an emphasis on purpose specification and use versus collection and data minimization as previously discussed.

In fact, Yahoo! has participated in the Advertising Options Program in part because it is an easy, one-stop shop for controlling OBA. 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.

4. Enforcement considerations

As mentioned above, appropriate enforcement mechanisms are key to successful self-regulation. The FTC has expertise in commercial data uses and enforcement and should continue as the lead enforcement agency in this regard. It can enforce against public declarations an entity makes that it will follow Codes of Conduct to the extent they apply to their business models. An entity can declare it is following a code, or more likely where online companies are concerned, will post in its privacy policy adherence to the code. Regulators can then hold the company to its commitments. State Attorneys General can further enforce these commitments.

Adherence to stated policies is also checked by NGOs – some including specific audits.²² These NGOs play a critical role in educating their industry members and in enforcing against codes of conduct. These efforts provide malefactors in industry an opportunity to learn and to quickly correct activity.

As there is further discussion about enforcement mechanisms, we cannot state strongly enough that trust in our word and our brand are essential to Yahoo!’s success with both consumers and advertisers.²³ Yahoo! has enormous incentives to hold itself accountable in the marketplace as well.

²² The Network Advertising Initiative requires internal audits. BBB Online has approved TRUSTe and Evidon as enforcement partners of the self-regulatory program for the Advertising Option Icon.

²³ 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

Finally, Yahoo! fully supports U.S. government efforts to work toward increased cooperation among privacy policymakers and enforcers across the globe. It is beneficial to recognize practical solutions to common problems even when operating under diverging privacy legal frameworks. In particular, Yahoo! supports a more focused and coordinated U.S. government representation of the U.S. position on privacy internationally, especially with the European Union as they undertake revision of the EU Data Protection Directive, and the development of a U.S. framework that furthers harmonization of privacy laws and enforcement. These efforts should yield benefits for consumers and to global businesses.

5. Legislative considerations

It is clear that Congress is also interested in protecting the privacy of Americans. Because the Working Group will be charged with assessing various proposals from lawmakers, we encourage you to consider the following practical points, but also to understand that Yahoo! strongly believes a self-regulatory approach enhanced by government enforcement is the best approach, resulting in timely innovations in privacy protections for consumers.

5.1 FTC should use reasonable criteria to evaluate Safe Harbors

Assuming Safe Harbor Frameworks are developed over time, it is important that the FTC have reasonable criteria to judge the acceptability of Safe Harbors incorporating the desire to encourage innovation while protecting privacy. Further, there must be some certainty that a Safe Harbor will apply for a reasonable period and that it will not be overturned. The FTC could review and approve a Code of Conduct or Safe Harbor while it is being developed, but should enforce against it only when the Code of Conduct or Safe Harbor has been adopted and put into operation. There may be a lag time between the time a code is adopted and the uptake by industry participants who will need to bring their practices and technology into alignment with the code. Reasonable time should be allowed for implementation, but industry should be put on notice that they will be able to avail themselves of the Safe Harbor benefits only when they make the required attestations.

5.2 Balancing criteria important in a FIPPs enforcement role.

If enforcement of FIPPs is restated separately from “unfair” and “deceptive” practices currently employed by the FTC, it is important that the offsetting or balancing criteria adhered to in its current evaluation of practices also be part of FIPPs evaluations. Any move toward FIPPs should not lose sight of these factors that account for countervailing benefits to consumers. Such evaluations are at the crux of innovative services. A new service may not be expected, or its benefit may not be entirely clear to a consumer, but in

time may provide benefits which are highly valued by users – either immediately or in the future.²⁴ If a strict FIPPs interpretation without balancing elements were to go into effect, new concepts for useful products and services will be suspect, or even illegal.

No overlap with sectoral laws

Yahoo! agrees that a sectoral approach has served us well, and that any additional privacy framework should not conflict with the sectoral laws already in place. However, these sectoral laws were put in place, in part, because they deal with the most sensitive data and users in our society. Any requirements for commercial privacy policies developed under new frameworks or legislation should not treat commercial data with stronger requirements than are present in existing law dealing with more sensitive data.

5.3 State uniformity

The inherently interstate nature, indeed the global nature, of the Internet makes doing business difficult in the absence of clear, harmonious legal principles. So that no one state can set policy for the others, it is very important that one national standard be implemented whenever possible, and to the extent feasible, global standards best reflect the modern demands of Internet architecture and services built upon it.

5.5 Private Rights of Action Should be Avoided

The Green Paper questions whether any future legislation should include a private right of action. Such a move would be a disproportionate response to any privacy concerns documented to date and would chill innovative and beneficial uses of data on widely-used websites. In more serious cases in which privacy interests were at stake, the FTC has reached agreements including notable civil penalties, which should be a first step if a more aggressive approach is warranted.

If a private right of action were the law of the land and a privacy violation were alleged, the sheer number of users on leading websites could result in hundreds or thousands of lawsuits. This threat could seriously discourage experimentation with data for beneficial features and functionality for consumers because one misstep could literally raise litigation costs to a point that threatens a business' viability. This chilling effect on beneficial features or functionality does not satisfy the goal of producing policy solutions that protect privacy while also promoting innovation.

²⁴ A good case study of this concept is the introduction of recommendations on Amazon.com. There was initial outcry over the service, but most people find it extremely helpful to get suggestions of interesting books today. Users can still turn off the feature.

5.6 Security breach legislation

Yahoo! agrees that a federal approach to legislation in the area of security breaches could be helpful—provided that such legislation supplants the myriad conflicting state laws that exist today and does not serve as a starting point for additional state rules that create further confusion about what is required. Because security breaches can lead to specific economic harm to consumers, Yahoo! has supported legislation to regulate disclosures of security breaches involving personally identifiable information that poses a significant threat of ID theft. Disclosure of breaches should be predicated upon the likelihood of potential harm from the breach.

5.7 ECPA Reform

The Electronic Communications Privacy Act (ECPA) has been in place since 1986 with two significant revisions in 1994 and 2001. ECPA covers both the lawful interception of communications and access to stored communications and data by government. Any initiative to revise ECPA must begin with the identification of specific shortcoming in the current statutory scheme, taking account of the extensive litigation that has occurred in recent years regarding the statute's scope and application. Yahoo! supports a careful assessment of the need to revise ECPA in light of currently available products, services and technologies that were not envisioned when it was enacted.

Again, thank you for the opportunity to comment on these critical issues. Yahoo! looks forward to continued discussions with the Working Group as it plays a vital role in the formation of policy in the weeks, months and years to come.

Respectfully submitted,



Anne Toth

Chief Trust Officer

Yahoo! Inc.