February 18, 2011

VIA ELECTRONIC DELIVERY

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"
File No. P095416

Dear Federal Trade Commission:

Facebook appreciates the opportunity to comment on the Federal Trade Commission's preliminary staff report proposing a privacy framework for businesses and policymakers. This framework, together with the privacy framework proposed by the Department of Commerce, represents a crucial effort on the part of the government to engage with stakeholders to develop a lens for understanding privacy. As we describe in these comments, we agree with the FTC and the Commerce Department that any privacy framework must be implemented in a way that both honors consumers' expectations in the contexts in which they use online services and promotes the innovation that has fueled the growth of the Internet over the past two decades.

In recent years, individuals have experienced a fundamental shift in the way that they use the Internet, with recent innovations allowing them to communicate and receive customized information in ways that could scarcely have been imagined just a decade ago. As the FTC report acknowledges, the diversity of this "social web" requires a reexamination of how industry and regulators understand privacy. Indeed, certain aspects of the social web—including those provided by Facebook—exist precisely because people want to share rather than limit the sharing of their information with others. The FTC's reexamination of privacy therefore must not only balance the public's demand for new and innovative ways to interact and share information against their interest in maintaining control over that information, but do so against a backdrop of continually evolving privacy expectations and preferences.

For Facebook—like most other online service providers—getting this balance right is a matter of survival. If Facebook fails to protect the privacy of its users adequately, those users will lose trust in Facebook and will stop using the service. At the same time, imposing burdensome privacy restrictions could limit Facebook's ability to innovate, making it harder for Facebook to compete in a constantly evolving industry. Fortunately, the FTC has expressly emphasized the importance of updating

1601 South California Avenue, Palo Alto, California 94304
650.543.4800 - tel 650.543.4801 - fax

our nation's consumer privacy framework to "tak[e] a flexible and evolving approach to privacy protection, designed to keep pace with a dynamic marketplace."[1]

These important goals—protecting privacy while promoting innovative services that enrich the online experience—have been the subject of much discussion, involving both the public and private sectors, over the past few years. This discussion has heightened awareness, empowered users, and prompted businesses to act responsibly. Although the privacy debate frequently is characterized as a contentious issue, in fact the areas of consensus far exceed the remaining areas of disagreement. Indeed, in reviewing the frameworks developed by the Commission and the Department, and after engaging with other stakeholders on privacy issues over the past several years, Facebook observes that the privacy debate and the proposals advanced by the FTC and the Commerce Department share a common focus on the following three main principles:

1. **Integrated Privacy Protections**: Companies should incorporate context-sensitive privacy protections throughout their organizations and products.

2. **Individual Empowerment and Responsibility**: To enable individuals to make the privacy decisions about information that are right for them, companies should provide a combination of greater transparency and meaningful choice appropriate to the context in which information is collected.

3. **Industry Accountability**: Robust industry self-regulatory efforts, in combination with judicious enforcement by the FTC, can address users' privacy concerns while providing sufficient flexibility to accommodate rapidly developing technologies and user expectations of privacy.

Facebook agrees that these three principles should be central to any effort to understand privacy in today's interconnected environment. But Facebook also believes that a framework based on these principles must be informed by two key insights reflected in both reports: (1) the importance of ensuring that privacy protections benefit, rather than frustrate, users' needs and expectations in the particular contexts in which they are implemented, and (2) the need for any privacy framework to promote rather than stifle the innovation that has been so essential to our economy.[2]

---

[1] Fed. Trade Comm'n, Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* 3 (Dec. 1, 2010) [hereinafter FTC Report]; *see also* Internet Policy Task Force, Dep't of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* iii (Dec. 16, 2010) (discussing the importance of updating our nation's consumer privacy framework to reflect "the digital economy's complexity and dynamism" in a way that will "allow innovation to flourish while building trust and protecting a broad array of other rights and interests") [hereinafter Commerce Report] .

[2] *See, e.g.*, President Barack Obama, State of the Union Address (Jan. 25, 2011) ("What we can do—what America does better than anyone else—is spark the creativity and imagination of our people. We're the nation that put cars in driveways and computers in offices, the nation of Edison and the Wright brothers, of Google and Facebook. In America, innovation doesn't just change our lives. It is how we make our living.").

This letter incorporates key elements from both the FTC and Department of Commerce proposals and describes how a framework based on the three principles that underlie them can serve as the basis of a dynamic privacy framework that will accommodate the changes yet to come. This discussion is intended to help frame our responses to the specific questions raised for comment in the preliminary FTC staff report, which are contained in the attached submission.

Facebook hopes that these comments, together with those of consumer groups, businesses, and other key stakeholders, will provide a basis for continuing the vital discussion initiated by the reports regarding an updated approach to privacy.

I. BACKGROUND

The Internet has evolved from an impersonal, one-dimensional medium into an interactive social platform where users have the power to shape their online experiences. The dynamic nature of the Internet requires an equally dynamic understanding of online privacy.

A. The Rise of the Social Web

Over the past several years, we have experienced a paradigm shift in the products and services available over the Internet. Just a decade ago, most Internet users consumed content that was static; their interactions were limited to emails, instant messages, product orders, and similar communications. Today, users enjoy access to a far more personalized and interactive Internet—the social web—that allows them to share their online experiences with friends and people around them and to receive online content that is tailored to them individually.

The growth of the social web allows Facebook's more than 500 million active users, at no charge, to instantly connect and share their information. For example, Facebook lets people share photographs with others through a feature that, with 86.9 billion images at last count, is the largest photo archive in the world. Through Facebook Platform, this social, personalized experience can be extended to other websites. For example, Bing uses Facebook Platform to enable users to receive customized search results based on content that their friends have "liked." These personalized services valued by users around the world are only the tip of the iceberg. Online service providers continually find new ways to add richness and depth to our online interactions.

The openness of the social web also has enabled people to connect not just with friends but with others who share common interests. For example, social media has played a key role in promoting democracy and civic engagement in the United States and abroad. In government, leaders use social media services to promote transparency, as evidenced by the nearly 140,000 followers of the White House Press Secretary's Twitter feed and the fact that more than 70 federal agencies have Facebook pages. Similarly, because social technologies enable users to quickly share information and build communities, democratic organizers have embraced them as key tools for engagement. Advocates of democracy used Twitter to make their voices heard following the contested 2009 Iranian election,[3] and Oscar Morales in Colombia famously employed Facebook to organize massive street

[3] Lev Grossman, *Iran Protests: Twitter, the Medium of the Movement*, TIME, June 17, 2009.

demonstrations against the FARC terrorist group in 2008.[4] Most recently, people in Tunisia and Egypt used social media to spread up-to-the-minute news, share videos of local events with the broader population, and mobilize online communities of thousands (and sometimes millions) behind a common cause.[5] This demonstrates that Facebook's model of encouraging sharing can provide tremendous benefits.

Quite apart from these examples, social media promote democracy because they strengthen civil society and the public sphere and thus help lay the groundwork for democratic trends to emerge. As Clay Shirky explains in his recent *Foreign Affairs* article, "social media's real potential lies in supporting civil society and the public sphere—which will produce change over years and decades, not weeks or months."[6]

Finally, the social web is a crucial engine for economic growth and job creation. Hundreds of thousands of application developers have built businesses on Facebook Platform. To take just one example, games developer Zynga, creator of the popular Farmville game, has more than 1,300 employees and has been valued at about $5.8 billion.[7] The social web also facilitates the sharing of information among friends, allowing people to discover new music, movies, and countless other products. Thanks to these innovations, the digital economy remains a vital source of jobs, growth, and investment, even in these challenging times.

B. The Dynamic Nature of Privacy on the Social Web

Justice Louis Brandeis may have famously defined privacy as "the right to be let alone," but—as the staff report acknowledges—"the application of this concept in modern times is by no means straightforward."[8] That is particularly true when it comes to social networking platforms like Facebook, which exist precisely so that users, far from being left "alone," can connect with others, build communities, and share details about their thoughts, interests, and activities on a regular basis. A better conception of privacy in the coming age is control over the "digital me."

---

[4] Sibylla Brodzinsky, *Facebook Used to Target Colombia's FARC with Global Rally*, CHRISTIAN SCI. MONITOR, Feb. 4, 2008.

[5] Alexis Madrigal, *The Inside Story of How Facebook Responded to Tunisian Hacks*, ATLANTIC, Jan. 24, 2011 (describing Facebook's rapid response to attempts by the Tunisian Internet censor to compromise dissenters' Facebook accounts); David D. Kirkpatrick & Jennifer Preston, *Google Executive Who Was Jailed Said He Was Part of Facebook Campaign in Egypt*, N.Y. TIMES, Feb. 7, 2011 (describing activist Wael Ghonim's role in setting up a Facebook page that became a tool for organizing protests and providing regular updates about other cases of police abuse).

[6] Clay Shirky, *The Political Power of Social Media: Technology, the Public Sphere, and Political Change*, FOREIGN AFF., Jan./Feb. 2011.

[7] Zynga Inc., *Fact Sheet*, http://www.zynga.com/about/facts.php (last visited Jan. 27, 2011); Michael J. de la Merced, *Zynga I.P.O. Is Said to Be Unlikely in 2011*, N.Y. TIMES DEALBOOK (Jan. 9, 2011, 9:15 PM), http://dealbook.nytimes.com/2011/01/09/public-offering-said-to-be-unlikely-for-zynga-this-year/.

[8] FTC Report i; *see also* NASA v. Nelson, 526 U.S. __ , slip op. at 11–17 (2011) (assuming, without deciding, that a constitutional right to informational privacy exists, employees' privacy interests were not implicated where government's inquiries were reasonable when "considered in context").

Given the vast difference between Justice Brandeis's conception of privacy and the way the concept applies to users on the social web, privacy cannot be viewed in one static way across every interaction that a user might have. Instead, an effective framework for privacy on the social web must focus on users' expectations, which depend on the nature and context of the relationships that users have with the companies and other services with which they interact.

Similarly, any new privacy framework must be sufficiently robust to account for the fact that technology and online services will continue to develop after the framework is finalized—and, with them, user expectations will develop as well. As the Department of Commerce rightly notes, "the pace at which consumers form expectations about acceptable and unacceptable uses of personal information is [now] measured in weeks or months."[9] Users' expectations with regard to privacy evolve rapidly, and so too must the controls that companies build to respond to those expectations.

At Facebook, building the services our users demand requires us to honor our users' desire to express themselves as well as their interest in controlling the information that they share on Facebook. The U.S. government should be mindful that achieving this balance is one of the greatest challenges facing the development of the social web. We, like other online service providers, must be acutely sensitive to evolving norms around privacy: Failing to protect our users' privacy will cost us the trust that is the foundation of the social web and will prompt our users to go elsewhere, but adopting overly restrictive policies will interfere with the social experience that is at the core of our services. Restrictive policies may unduly limit individuals' expression and control over their digital selves, which they wish to present to the world. Thus, to adequately meet our users' expectations, we not only need to identify and propose solutions where protections are needed; we also need to recognize those places where privacy protections are unnecessary or even cumbersome. And we need to evolve our services—including the privacy protections that we implement—in response to the feedback that we receive from our users.

Facebook's goal is to develop innovative products that facilitate sharing, self-expression, and connectivity, and also protect privacy by giving users greater control over the information they share and the connections they make. We believe our demonstrated ability to inspire trust in our users while continuing to pioneer new online services makes us well suited to contribute to the government's inquiry into the future of privacy.

II. INTEGRATED PRIVACY PROTECTIONS

The privacy frameworks proposed by the FTC and Commerce Department recommend that companies consider privacy issues systematically, building robust privacy protections into the design process and throughout their organizations. The FTC staff refers to this principle as "privacy by design," while the Commerce Department highlights this as part of a larger transparency principle that would encourage privacy impact assessments ("PIAs") among other measures.[10]

---

[9] Commerce Report 47.

[10] FTC Report 44; Commerce Report 34–36.

A. Robust Privacy Safeguards

Facebook understands that the social web can exist only in an environment of trust—trust among users as well as trust between users and their online service providers. As part of its commitment to protecting privacy and in order to ensure that privacy is being considered everywhere in the company, Facebook has implemented a number of privacy safeguards. These include a Chief Privacy Counsel and other dedicated privacy professionals who are involved in and review new products and features from design through launch; privacy and security training for employees; ongoing review and monitoring of the way data is handled by existing features and applications; and rigorous data security practices.

Facebook also incorporates contextual privacy controls into its product offerings. Because Facebook's users expect and demand innovative features that allow them to connect with other people in creative new ways, we constantly strive to develop better methods for users to communicate with each other while maintaining control over the information that they share. In the past two years, Facebook built privacy controls into various aspects of our services, each designed to give users the ability to control how they present themselves and how they connect to others in the digital world.

- In July 2009, we launched a new publisher privacy control that allows users to select a specific audience (or even customize the audience) every time they post content on Facebook. By clicking a simple lock icon, a user can, for example, post a status update to everyone, and then limit distribution of a photo to just her family.

- In December 2009, we introduced a new privacy framework and took the unprecedented step of requiring all users to evaluate and select their privacy settings before they could continue using Facebook's services. Hundreds of millions of users interacted with our Privacy Transition Tool to consider whether their settings accurately reflected their privacy preferences.

- In May 2010, we simplified our privacy settings. These new controls allow users to set their sharing preferences with one click or to customize their information sharing using more granular tools.

- In June 2010, we introduced a new process for authorizing third-party applications. Before a user installs a new application, we serve a dialog box that describes each type of information the application needs from the user, and asks the user to grant the application permission to access that information.

- In August 2010, we introduced what we believe to be a first-of-its-kind innovation where we provided people who use Facebook with the ability to set their privacy settings on their mobile devices and have those settings work across the entire Facebook experience, including on the Facebook.com site.

- In October 2010, we rolled out our application dashboard, which allows users to see the permissions they have given applications, as well as the last time each application accessed their information. It also allows users to remove applications they no longer want to access their information or remove certain permissions they have granted.

- Also in October 2010, we introduced a data export tool that makes it easy for users to download a file that contains every status update, photo, or other content they have posted to the site.

- In January 2011, we launched a series of privacy enhancing security tools that empower users to increase the security of their account. These tools include enabling https security for safer web access, and the ability for users to track log in access to their account and remotely log out.

B. A Contextual and Dynamic Approach

In developing these tools, we have learned that there is no one-size-fits-all solution with respect to safeguarding privacy. Rather, any approach to privacy must give due regard to the context in which the information is collected or used, which necessarily shapes users' privacy expectations. Further, the approach must account for individuals' widely varying attitudes regarding sharing of data, recognizing that there are some who want to share everything, some who want to share nothing, and that everyone else falls somewhere in between.

When considering integrated privacy practices, it is important to take into account the nature of the user's relationship with the service provider and the difference that makes to the user's need for privacy. For example, shoppers know that security cameras capture images of them when they enter a store, but they normally expect that the store will not retain its recordings after it becomes clear that they are not needed for law enforcement purposes. But the many users who treat Facebook or another social networking service as the central point for storing their status updates, photos, videos, events, and links and sharing them with their friends have different expectations. These users essentially view Facebook as their personal digital archives, and they expect Facebook to preserve this valuable information and keep it safe. This basic expectation drives our security and retention practices.

It is also important to acknowledge that information originally collected for one purpose can sometimes be reused in entirely new, creative ways that ultimately benefit users. Regulations that restrict such new uses of information stifle innovation to the detriment of consumers. Consider, for example, the development of the following services:

- **Caller ID.** Telephone companies originally collected and exchanged subscribers' telephone numbers solely for the purpose of completing telephone calls. But telephone companies later realized that they could use this information to display the calling party's telephone number and name to the call recipient, allowing the recipient to identify the caller in advance. Today, caller ID is an accepted and valued part of telephone communication, and few subscribers choose to block outgoing caller ID even though it is easy to do so.

- **History-Sensitive Hyperlinks.** Mosaic and other early web browsers collected information about the pages that a user visited exclusively for the purpose of retrieving and delivering those pages. But developers quickly realized that browsers could record a user's browsing history and change the color of already-visited hyperlinks in order to aid in navigation. Today, modern browser users have the ability to disable recording of their browsing histories, but most view this functionality as a basic part of the online experience.

- **Netflix.** When Netflix first introduced its DVD-rental-by-mail service, it collected information about users' movie preferences in order to send users the specific videos they requested. This information later became the foundation of the personalized video recommendation engine that is now one of Netflix's most compelling features.

- **Amazon Recommendations.** At its inception, Amazon's website simply listed products available for sale and collected information about customers' website choices in order to fulfill orders. But Amazon now uses purchasing and browsing history to generate recommendations for products in which users might be interested. Again, although users have the ability to disable this feature, most choose to retain it because of its perceived value.

- **Facebook News Feed.** In 2006 Facebook launched a new feature called News Feed on every person's homepage. The product updated a personalized list of news stories throughout the day so users would know what their friends were posting. Before News Feed, people had to visit their friends' profiles to see what their friends were up to. Despite initial user skepticism when the product was first launched, News Feed is now—as any user would attest—an integral part of the Facebook experience.

- **Google Flu Trends.** When the founders of Google began collaborating on a search-engine research project in 1996, they probably did not envision that search queries about flu-related topics would one day become an early detection system for flu outbreaks. Today, Google Flu Trends can estimate flu activity one to two weeks more quickly than traditional surveillance systems involving virologic and clinical data, and may help public health officials and health professionals better respond to seasonal epidemics.

As technology advances, individuals understand that their data may be used or made available in new ways.[11] In the digital world in particular, users have come to understand and even expect that services will evolve and that companies will offer innovative new features that improve the online experience. The Department of Commerce's report, recognizing that creative reuses of existing information can lead to innovation but also cautioning that such innovative reuses should not come at the expense of user privacy, recommends a nuanced approach to the issue—one that weighs the benefits of the particular reuse against the harms and calibrates notice and consent requirements accordingly.[12] Facebook believes that such an approach is necessary in light of the many examples of reuse that have provided immense benefits to the public while producing little if any discernible harm.

---

[11] For instance, following 1995 legislation authorizing electronic filing of campaign finance reports, the Federal Election Commission began allowing visitors to its website to search a database of individuals' reported federal campaign contributions. *See* Federal Election Campaign Act of 1971, Amendment, Pub. L. No. 104-79, section 1(a), 109 Stat. 791 (Dec. 28, 1995) (requiring the FEC to "permit reports required by this Act to be filed and preserved by means of computer disk or any other electronic format or method, as determined by the Commission"). The FEC determined that this innovation served the public interest even though it involved the use of information about individuals in a new way.

[12] Commerce Report 38–39.

III. INDIVIDUAL EMPOWERMENT AND RESPONSIBILITY

Facebook agrees with the FTC and the Commerce Department that individuals should be empowered to control the ways in which information about them is used and to take responsibility for the choices that they make. As each agency's report acknowledges, however, a privacy framework cannot assume that the same rules and practices apply to all people in all contexts.[13] Context-inappropriate privacy restrictions can frustrate, rather than promote, users' interests and expectations. Instead, offering a combination of transparency and choice is the best way to empower individuals to make the privacy choices that are right for them in the context of the particular information that they are choosing to share.

A. Transparency

Both agencies agree: what users need is not more information, but clearer and more meaningful information. At Facebook, we likewise are committed to making privacy disclosures more helpful to our users. Consistent with the FTC staff's suggestion that privacy notices should provide "clear . . . and concise descriptions of a company's overall data practices,"[14] we completely rewrote our privacy policy in October of 2009 to make it easier for users to understand our policies and practices, and we are continuing to work to find more user-friendly and less legalistic ways to convey key information to our users. We also give mobile users access to most of the privacy settings available to them on the web, enabling them to make real-time choices about the data they share, even when accessing Facebook on the go.

Facebook also agrees with the FTC staff's recommendation that privacy notices should be easier to compare. One way to help users compare entities' privacy practices—while avoiding the problems associated with rigid disclosure standards—would be for companies or self-regulatory groups to develop model privacy notices that describe the general practices in a specific industry (such as social networking services or e-commerce sites). Individual companies then could augment these common privacy notices by publishing supplemental statements, found in a standard place on their websites, that detail any practices that are not described in, or deviate from, the model notice. This would allow users to compare privacy practices across companies within an industry without unduly limiting the disclosure itself, as would likely happen if companies were constrained to make disclosures using standardized "check boxes" that do not leave room for meaningful descriptions of a specific entity's practices.

While transparency is important, it must be implemented with due regard for the rapidly changing nature of online services and the realization that overly restrictive obligations hinder innovation. For example, the staff recommends that companies obtain affirmative consent from users before using previously-collected data in a "materially different manner" than described in an earlier

---

[13] *See, e.g.*, FTC Report 54 ("Staff believes that requiring consumers to make a series of decisions whether to allow companies to engage in these obvious or necessary practices would impose significantly more burden than benefit on both consumers and businesses."); Commerce Report 13 ("Public policy can help establish trust not only by defining obligations but also making available information that helps individuals decide whether to entrust another person or entity with personal information.").

[14] FTC Report 71.

privacy notice.[15] While Facebook agrees that notice and consent may be appropriate for certain changes in data practices, it is essential to avoid interpreting the term "material" too restrictively. A restrictive interpretation could prevent companies from launching new features out of an uncertainty about whether those features would use data in a "materially different manner." Such an interpretation might have prevented features like the caller ID displays and Netflix recommendations described above from ever having been offered—a result that could hurt the future of the digital economy.

A restrictive material change obligation also would have the perverse effect of creating a race to the bottom—undermining the purposes of the proposed frameworks by encouraging companies to be *less* protective of users' privacy. This is because disclosure of uses would become a one-way ratchet: companies that initially disclosed no user privacy protections at all would be free to use data in expansive ways, while companies that provided more transparency and choice at the outset could have difficulty modifying their services to implement new technologies or offer other benefits out of a concern that those changes would be deemed "material." In short, a restrictive interpretation would disadvantage existing companies in competition with new entrants and would encourage those new entrants to offer few privacy protections in the first instance.

In addition, while notice and consent for certain changes may be appropriate, it is essential that any consent requirement be context-sensitive. For instance, depending on the context, the best way to obtain consent may be to require users to accept a disclosure before continuing, whereas in other situations an individual's continued use of a service after a service provider offers a prominent opt-out opportunity may be a more meaningful approach. As the staff observes, "a clear, simple, and prominent opt-out mechanism may be more privacy protective than a confusing, opaque opt-in."[16] The FTC report also endorses in some situations the use of "a 'just-in-time' approach, in which the company provides the consumer with a choice at the point the consumer enters his personal data or before he accepts a product or service."[17] Indeed, as the staff concludes, making it easy for users "to understand and exercise their options may be more relevant . . . than whether the choice is technically opt-in or opt out."[18]

Ultimately, the FTC's enforcement activities in the area of privacy must be guided by the realization that aggressive enforcement and imprecise standards can lead to more legalistic disclosures—and, as described above, chill economic growth—as companies seek to manage regulatory risk by over-disclosing, reserving broad rights, and under-innovating. To avoid these unintended consequences, the FTC should err on the side of clarifying its policies rather than taking aggressive enforcement action against practices that previously were not clearly prohibited.[19] In this regard, as the

---

[15] FTC Report 77.

[16] FTC Report 60.

[17] FTC Report vi.

[18] FTC Report 60.

[19] As we discuss further below, the FTC has long recognized the importance of a restrained approach to enforcement and has, accordingly, only exercised its authority under the FTC Act in limited circumstances (*i.e.*, upon a finding of "substantial injury" to consumers or that "injury is likely") and, furthermore, has only acted after weighing the costs and benefits of its intervention.

Commerce report notes, it is important to consider whether the change is likely to bring social benefits that users want.[20] Where a user has an existing relationship with a business and the change will benefit the user through new or innovative service offerings, opt-in consent should not be required. In such instances, a company instead should be able to inform users in advance about how the company will notify them of material changes—such as on a standardized place on its website or through email—and then allow users sufficient time to opt out, share less information, or close their account before the change takes effect.

B. Choice

As both the FTC and Commerce reports emphasize, enhanced transparency is important to individual empowerment because it helps people make better informed choices when deciding whether to entrust someone else with information about themselves.[21] But empowering individuals also involves giving them the ability to choose how the information collected about them should be used once it is collected.

User control is an essential component of Facebook. As discussed above, we provide users with the ability to choose a specific audience every time they post content, and we require applications to obtain express permission before accessing any information beyond that which is publicly available.

Much like transparency, choice should be treated under any privacy framework in a way that is sufficiently flexible to account for the speed of innovation on the Internet and the accompanying changes in users' expectations. For example, the FTC staff proposes that "just in time" notice should not be required when an entity collects information for what the staff calls a "commonly accepted practice."[22] Facebook agrees that notice would be inappropriate and deemed intrusive when disclosures concern uses of information that users already expect based upon the context in which the information is collected.

However, the concept of "commonly accepted practices" must be based on *users'* expectations in using a particular service, not on expectations included in regulations or policy statements, which are likely to be updated long after any new technology or service has gained currency among users. And the concept should be construed in a way that adequately accounts for the way users' expectations shift over time. As recently as the mid-1990s, Internet users were reluctant to engage in financial transactions online. Yet the FTC report recognizes online product and service fulfillment as a commonly accepted practice today. This demonstrates the error of attempting to implement prescriptive standards in advance of developing technology, an overbroad practice that ultimately risks stifling innovation without any countervailing public interest benefit.

---

[20] Commerce Report 39 (recognizing that reuse of data, even if contrary to the service provider's specified purposes for collecting the information in the first place, "may actually add value that the user appreciates").

[21] Commerce Report 13; FTC Report 58–60.

[22] FTC Report 53–55.

One promising option for implementing choice may be the adoption of "do not track" functionality, which the FTC staff proposed in the context of entities that use invisible web beacons, cookies, or similar technologies to collect behavioral information about users with whom they do not have a direct relationship for ad targeting purposes. But it is essential that any "do not track" implementation specifically define what "tracking" is prohibited. For instance, web servers routinely collect client computers' IP addresses in order to communicate with them and receive requests to deliver specific web pages to particular addresses. Similarly, a website may use historical login data that it has collected for account security purposes, such as the additional account security questions that Facebook would ask a user who always logged in from Washington, D.C. if we suddenly see failed login attempts on that account from Belarus. While these collections of information might be defined as "tracking," they are clearly not practices that users would intend to block by expressing a "do not track" preference. To the contrary, they are inherent in the structure and proper functioning of Internet services.

Instead, the staff's "do not track" proposal rightly focuses on the data practices of entities that do not directly engage with users, and that thus are not accountable to users. In these situations, a user may not know that an entity is collecting information about her, may not have a place to look to learn more about that entity's data practices, and may have no recourse if she objects to those practices after learning of them. Because of these difficulties, a "do not track" mechanism provides a meaningful way for a user to express her preference not to share information with entities that she does not know.

In contrast, information collection by a company with which a user has a relationship and whose presence on a webpage is clear does not present the same concerns because the user expects that the entity may be collecting data. The user also can more easily learn about the data collection and provide feedback, share less information, or terminate the relationship altogether. Finally, users can seek redress if they object to an approach taken by a company they know: among other steps, they can complain about that company by name to Congress or the FTC or try to force a reduction in that company's stock price through grassroots public relations efforts. None of these corrective measures are available for "no-name" companies that are invisible to the Internet users from whom they collect data.

A contextual "do not track" approach that recognizes these differences in user expectations, and that adopts bifurcated requirements for companies depending on whether they are known to and interact directly with users, is consistent with the FTC's approach to Do Not Call, which similarly contains an exception for established business relationships.[23]

---

[23] 16 C.F.R. § 310.4(b)(1)(iii)(B)(ii) (permitting an entity to make calls to a telephone number included in the national "do-not-call" registry if it has an established business relationship with the call recipient).

IV. INDUSTRY ACCOUNTABILITY

In their reports, the FTC and the Commerce Department highlight the need to hold companies accountable for their privacy practices.[24] Facebook agrees that industry's willingness and ability to respond to and correct practices to which users object is essential to building trust. While we believe that the interactive and competitive nature of the social web provides companies with sufficient incentives to be responsive to user concerns, we recognize that voluntary, enforceable codes of the kind recommended by the Department of Commerce may provide a valuable backstop in those instances where users' expectations are not being met. We also agree that thoughtful regulatory action can help redress tangible harms caused by unfairness and deception in companies' handling of user data.

A. Accountability Through Self-Correction and Self-Regulation

The social web encourages user input and responsive self-correction. Consistent with Facebook's role as a platform built on the sharing of information, we have implemented numerous channels to facilitate feedback from our users. Indeed, Facebook's efforts to engage with its users on changes to its privacy policy or information sharing practices are virtually unparalleled in the industry. For example, when we make changes to our privacy policy, we announce them broadly and give users the ability to comment on the proposed changes (unless the changes are administrative or required by law). We are the only major online service provider that allows users to vote on the changes if comments reach a pre-set threshold. And we take the input that we receive from our users seriously. Time and again, Facebook has shown itself capable of correcting course in response to user feedback and thereby continuing to build trust.

While, as the FTC report states, "industry must do better" in protecting privacy,[25] private-sector efforts are particularly well suited for solving privacy-related problems on the Internet. This is because private-sector initiatives generally can respond quickly to changing technologies and evolving online business and social practices. In addition, private-sector mechanisms, because they are user-driven by nature, are more likely to permit users to choose among various solutions based on their individual privacy preferences.

Over the past several years, industry has shown itself capable of providing innovative solutions to the Internet era's most vexing privacy issues. For example, the late 1990s and early 2000s saw ISPs and email inboxes overrun with junk email. Although the federal CAN-SPAM Act may have curbed some of the spammers' worst abuses, it is the ISPs' development of sophisticated mail filters that has most effectively addressed the problem of spam. Industry also has responded to government concerns about privacy. After the release of the FTC's 2009 staff report on online behavioral advertising, the advertising industry created the Self-Regulatory Principles that now provide users with unprecedented control over the use of browsing data for third-party behavioral targeting purposes. Already, the publishers of the three most popular web browsers—Microsoft Internet Explorer, Mozilla

---

[24] *See, e.g.*, FTC Report 70 (noting the importance of privacy policies in making companies accountable for their practices); Commerce Report 40 (observing that auditing and accountability "play a critical role" in ensuring that "organizations follow the practices to which they are bound").

[25] FTC Report i.

Firefox, and Google Chrome—have announced functionality that responds to the FTC staff's suggestion that browsers implement "do not track" features.

Facebook agrees that the efforts of individual companies can be supplemented, as the Department of Commerce suggests, by industry codes of conduct that address the unique aspects of the many different kinds of services on the web. Sector-specific codes, unlike slow-paced legislation or agency rules, can be updated quickly to accommodate rapidly developing technologies and user expectations of privacy. In the ever-evolving world of online services, specificity and adaptability are essential to preserving the kind of accountability that users demand.

At the same time, Facebook recognizes that more concerted activity may be necessary to continue to make progress on the privacy front. For this reason, Facebook supports the Commerce Department's recommendation to establish a Privacy Policy Office that would bring stakeholders together to find mutually acceptable solutions.

B. The Role of Government Regulation

Context-sensitive regimes that promote user control and industry self-correction should be the primary means of protecting user privacy online, but this is not to say there is no role for government regulation in this space.

Although Congress has been hesitant to interfere in this area—out of a proper concern for dampening the creative forces that drive the Internet as well as infringing the freedom of speech protected by the First Amendment—it has enacted targeted legislation that protects against tangible harms stemming from online misconduct. For instance, in certain circumstances, COPPA penalizes the collection of data from children absent parental consent out of concern for children's online safety. And the CAN-SPAM Act protects against the harm caused by the high percentage of spam emails that contain false or misleading statements.

The FTC, as the principal enforcer of industry's privacy obligations to the public, has been charged by Congress to take enforcement action in response to "unfair" trade practices only if those practices "cause[] or [are] likely to cause substantial injury to consumers."[26] Consistent with this congressional directive, the FTC brings enforcement actions for deceptiveness only after determining that a deception was "material" and that, therefore, consumer "injury is likely."[27] Accordingly, in exercising its enforcement authority under Section 5 of the FTC Act, the agency has focused on practices that have the potential to do real harm to individuals, such as through identity theft and material misrepresentations about data practices.[28]

---

[26] 15 U.S.C. § 45(n).

[27] Letter from James C. Miller III, Chairman, FTC, to Hon. John Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983), appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984) ("FTC Policy Statement on Deception").

[28] For example, the FTC's recent deceptiveness settlement with the popular social networking service Twitter was based on the agency's allegation that Twitter had "falsely represent[ed] to consumers that it use[d] at least reasonable safeguards to protect user information from unauthorized access" and its (continued...)

This measured approach to enforcement reflects the Commission's considered judgment that "normally, . . . the marketplace [is] self-correcting" and people can be expected to make choices in their best interests.[29] The Commission therefore interprets its unfairness authority as extending only to those practices that "may prevent consumers from effectively making their own decisions."[30] Similarly, the materiality consideration under Section 5's deceptiveness prong limits the Commission's enforcement authority to regulating those acts or omissions that are "likely to affect a consumer's choice of or conduct regarding a product."[31]

The FTC also has recognized that its efforts to protect choice must not be exercised in a way that stifles innovation by imposing undue burdens on businesses without providing an equivalent public benefit. Facebook urges the Commission to continue to pursue a restrained approach to enforcement, carefully considering the costs of any intervention so that its efforts will not unduly interfere with companies' ability to innovate and evolve the services they make available to users.

V. CONCLUSION

Facebook applauds the Commission and the Commerce Department for their work in developing an updated framework for protecting privacy in a way that encourages the growth of innovative new services. We believe that both reports contain the essential principles that, taken together, can serve as the basic building blocks for a meaningful reevaluation of our approach to privacy in the United States. We also agree with the FTC's observation that any privacy framework must be *dynamic*. By implementing the principles in a way that accommodates the evolving and often unpredictable privacy norms of the twenty-first century, we can create a framework that is sensitive to the different expectations of privacy users have in different contexts, maximizes users' ability to control their privacy as they see fit, and promotes continued innovation.

Respectfully submitted,

Michael Richter
Chief Privacy Counsel
Facebook, Inc.

---

finding that Twitter's failure to implement those safeguards had resulted in intruders "(1) gain[ing] unauthorized access to nonpublic tweets and nonpublic user information, and (2) reset[ting] users' passwords and send[ing] unauthorized tweets from users' accounts." *In re Twitter, Inc.*, Analysis of Proposed Consent Order to Aid Public Comment, File No. 0923093, at 1-2, Jun. 24, 2010, available at http://www.ftc.gov/os/caselist/0923093/100624twitteranal.pdf.

[29] *See* Letter from Michael Pertschuk, Chairman, FTC, to Hon. Wendell H. Ford, Chairman, Sen. Consumer Subcomm., and Hon. John C. Danforth, Ranking Member, Sen. Consumer Subcomm. (Dec. 17, 1980), appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) ("FTC Policy Statement on Unfairness").

[30] *Id.*

[31] *See* FTC Policy Statement on Deception.

Enclosure

FEBRUARY 18, 2011

RESPONSES TO FEDERAL TRADE COMMISSION STAFF QUESTIONS

"PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS"

Facebook appreciates the opportunity to submit these responses to the questions that the FTC staff raised in their preliminary report on a new framework for protecting consumer privacy. To facilitate review, our responses address many of the questions raised by the staff and follow the same order as the topics addressed on pages 42 through 79 of the report.

Scope

- *Are there practical considerations that support excluding certain types of companies or businesses from the framework – for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?*

- *Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"?*

- *How should the framework apply to data that, while not currently considered "linkable," may become so in the future?*

- *If it is not feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device," what alternatives exist?*

- *Are there reliable methods for determining whether a particular data set is "linkable" or may become "linkable"?*

- *What technical measures exist to "anonymize" data and are any industry norms emerging in this area?*

The staff report, noting the diminishing importance of the traditional distinction between personally identifiable information and non-personally identifiable information, suggests that the proposed privacy framework cover all data that can be "reasonably linked to a specific consumer, computer, or other device."[32] Facebook understands that users have privacy interests that may be implicated even when information about them is not specifically tied to their name, address, or other personal contact information. However, the privacy protections to be extended to data should depend on context (e.g., the type of data, and the relationship between the individual and the business).

---

[32] FTC Report 43.

The report also proposes a uniform framework that would apply to both the online and offline collection of data. Our comments focus on issues surrounding online privacy, although we recognize that offline data practices may also raise user privacy concerns. A privacy framework that purports to cover both online and offline data will only be workable if it reflects the significant contextual differences between online and offline interactions and takes into account users' expectations regarding their relationships with the specific entities with which they deal.

Consumer privacy throughout the organization: incorporating substantive privacy protections

- *Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?*

- *Should the concept of "specific business purpose" or "need" be defined further and, if so, how?*

- *Is there a way to prescribe a reasonable retention period?*

- *Should the retention period depend upon the type or the sensitivity of the data at issue? For example, does the value of information used for behavioral advertising decrease so quickly that retention periods for such data can be quite short?*

- *How should the substantive principles set forth in Section V(B)(1) of the report apply to companies with legacy data systems?*

- *When it is not feasible to update legacy data systems, what administrative or technical procedures should companies follow to mitigate the risks posed by such systems?*

- *Can companies minimize or otherwise modify the data maintained in legacy data systems to protect consumer privacy interests?*

Facebook agrees that the adoption of integrated privacy protections throughout an organization can help safeguard user privacy. However, such privacy protections must take into account the fact that users expect online services to evolve and innovate. In particular, an overly restrictive reading of "specific business purpose" that denies companies the flexibility to adjust their uses of information could prove harmful to the future of the Internet. Users often benefit when information is reused in creative ways that were unforeseeable when the information was initially collected, just as they did when telephone companies repurposed telephone directory information to develop caller ID. Subject to appropriate notice and consent requirements, companies should be permitted to alter their data-handling practices to incorporate new features and technologies that provide a net benefit to society.

Similarly, any limitations on data retention must take into account the nature of the user's relationship with the company. As discussed in our overview letter, shoppers normally expect that security camera footage will be deleted once the videos are no longer needed for law enforcement purposes, but they have different expectations when it comes to the information that they voluntarily share and archive on Facebook. For example, if a user uploads a photo on Facebook, the user expects that the photo will remain available until he or she chooses to remove it. As with other data handling practices, the reasonableness of a company's data retention policies must be assessed in context.

Consumer privacy throughout the organization: maintaining comprehensive data management procedures

- *How can the full range of stakeholders be given an incentive to develop and deploy privacy-enhancing technologies?*

- *What roles should different industry participants – e.g., browser vendors, website operators, advertising companies – play in addressing privacy concerns with more effective technologies for consumer control?*

In asking for input on how the full range of stakeholders can be encouraged to deploy technologies that will protect privacy, the staff implicitly and correctly acknowledges that there is no single solution that will convince all stakeholders to develop and implement comprehensive data management procedures. Facebook agrees that different incentives may be needed for different participants, depending on the stakeholder's industry sector or role in the digital economy. For consumer-facing companies and for social networking sites in particular, user feedback is an incredibly powerful tool for self-regulation and self-correction. As discussed in our overview letter, Facebook has on numerous occasions modified our privacy practices to address user concerns.

All industry participants have roles to play in maintaining comprehensive data management procedures. As described above, we believe that service providers like us should furnish information to users about how information about them is collected and used and should give them tools to exercise choices concerning that information. At the same time, Facebook applauds the efforts of software vendors like Microsoft, which have announced implementation of choice tools that allow users to exercise choice at the browser level. Likewise, the partnership of the Direct Marketing Association, the Council of Better Business Bureaus, the Interactive Advertising Bureau, and others to develop the AboutAds.info website—which offers a unique industry-wide tool for users to learn more about the data that is being collected about them and to exercise choice—is an important illustration of the significant user benefits that can be developed through industry cooperation.

These examples illustrate that, even in the absence of government regulation, user empowerment and competitive pressure to improve the overall user experience provide strong incentives to deploy the privacy-enhancing technologies that users demand. These examples are just the beginning of the initiatives that various stakeholders will develop, and users will be well served by that innovation.

Choice: Commonly accepted practices

- *Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?*

- *Are there practices that should be considered "commonly accepted" in some business contexts but not in others?*

- *What types of first-party marketing should be considered "commonly accepted practices"?*

- *Even if first-party marketing in general may be a commonly accepted practice, should consumers be given a choice before sensitive data is used for such marketing?*

- *Should first-party marketing be limited to the context in which the data is collected from the consumer?*

    - *For instance, in the online behavioral advertising context, Commission staff has stated that where a website provides recommendations or offers to a consumer based on his or her prior purchases at that website, such practice constitutes first-party marketing. An analogous offline example would include a retailer offering a coupon to a consumer at the cash register based upon the consumer's prior purchases in the store. Is there a distinction, however, if the owner of the website or the offline retailer sends offers to the consumer in another context – for example, via postal mail, email, or text message? Should consumers have an opportunity to decline solicitations delivered through such means, as provided by existing sectoral laws?*

- *Should marketing to consumers by commonly-branded affiliates be considered first-party marketing?*

- *How should the proposed framework handle the practice of data "enhancement," whereby a company obtains data about its customers from other sources, both online and offline, to enrich its databases? Should companies provide choice about this practice?*

Facebook agrees that there are certain practices, such as fraud prevention, legal compliance, service delivery, and first-party marketing, that users expect to occur and for which it would be unnecessarily intrusive to interrupt users to disclose commonly understood practices and seek affirmative consent before users may proceed.

At the same time, any evaluation of "commonly accepted practices" must start from the realization that what is commonly accepted may vary depending on context. In his concurrence, Commissioner Kovacic asks how policymakers should go about identifying mainstream consumer expectations for purposes of setting default terms with respect to data collection and use. The challenges that policymakers face in identifying such expectations are compounded by the fact that different industries have different commonly accepted practices. For example, online publishers—as well as traditional publishers, like newspapers and magazines—have long provided contextual advertising based on the particular page of content that the user is viewing, and users generally are not concerned about this practice.[33] In contrast, financial institutions are only now starting to explore the possibility of providing offers and other targeted marketing material in users' bank statements.[34] Although novel now, contextual advertising in that context may eventually become a commonly accepted practice as well.

As discussed above, any attempt to define a set of commonly accepted practices also must take into account the fact that users' expectations evolve over time. Fifteen years ago, privacy and security concerns meant that most users hesitated to purchase items online. In contrast, during the 2010

---

[33] *See* FTC Report 55 n.134 (recognizing that online contextual advertising is more transparent to consumers and "should fall within the 'commonly accepted practices' category").

[34] *See* Ylan Q. Mui, *Banks Allow Ads in Online Checking Accounts*, WASH. POST, Jan. 17, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/16/AR2011011603387.html (discussing introduction of advertisements linked to recent purchases on consumers' online bank statements).

holiday season, online retail spending injected billions into the U.S. economy. Innovation and progress often require the development of new experiences that users may not have thought of, or may even initially reject but later come to appreciate. Many Facebook users protested the initial launch of News Feed, but it is now regarded as an essential component of the Facebook experience.

Moreover, static rules implemented in the face of advancing technology can quickly become outdated and stifle the development of promising new inventions. When steam-powered cars were introduced in England in the mid-eighteenth century, "the speed limit was hastily set at 4 miles per hour—the speed at which a man carrying a red flag could run ahead of a car entering town."[35] By the time the Red Flag Act was repealed in 1896, it had "effectively stifled the development of road transport in the British Isles."[36]

Finally, the report proposes that consent requirements should differ depending on whether the user is interacting with a "first party" or "third party." This distinction may not fully capture the many complex relationships that users have on today's Internet. As the Commerce Department recognizes in its complementary report, the rise of the social web means that the modern online experience often involves multiple companies providing content and services through a single interface.[37] For example, a user of Google Reader can personalize the service to display content from *USA Today* and the FTC's RSS feed, and can, with one mouse click, share particularly interesting articles on his or her favorite social networking site. This exchange of information—between users and multiple service and content providers—is essential to providing users with the interactive experiences that they demand. When assessing what level of consent is required, the inquiry should focus on (1) whether the company has an obvious presence on the page, and (2) whether the user has entered into a knowing and voluntary relationship with the company. Fewer privacy concerns are raised and less intrusive notice is required when the user understands which company is collecting the information and has other means of holding the company accountable for its information practices.

Choice: Practices that require meaningful choice

- *What is the most appropriate way to obtain consent for practices that do not fall within the "commonly accepted" category?*

- *Should the method of consent be different for different contexts?*

    - *For example, what are effective ways to seek informed consent in the mobile context, given the multiple parties involved in data collection and the challenges presented by the small screen?*

    - *Would a uniform icon or graphic for presenting options be feasible and effective in this and other contexts?*

---

[35] TOM VANDERBILT, TRAFFIC: WHY WE DRIVE THE WAY WE DO (AND WHAT IT SAYS ABOUT US) 10–11 (2008).

[36] Ken W. Purdy & Christopher G. Foster, *Automobile*, *in* ENCYCLOPEDIA BRITANNICA, http://www.britannica.com/EBchecked/topic/44957/automobile (last visited Feb. 17, 2011).

[37] *See* Commerce Report 37.

- *Is there market research or are there academic studies focusing on the effectiveness of different choice mechanisms in different contexts that could assist FTC staff as it continues to explore this issue?*

- *Under what circumstances (if any) is it appropriate to offer choice as a "take it or leave it" proposition, whereby a consumer's use of a website, product, or service constitutes consent to the company's information practices?*

- *What types of disclosures and consent mechanisms would be most effective to inform consumers about the trade-offs they make when they share their data in exchange for services?*

  - *In particular, how should companies communicate the "take it or leave it" nature of a transaction to consumers?*

  - *Are there any circumstances in which a "take it or leave it" proposition would be inappropriate?*

- *How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?*

- *What additional consumer protection measures, such as enhanced consent or heightened restrictions, are appropriate for the use of deep packet inspection?*

- *What (if any) special issues does the collection or the use of information about teens raise?*

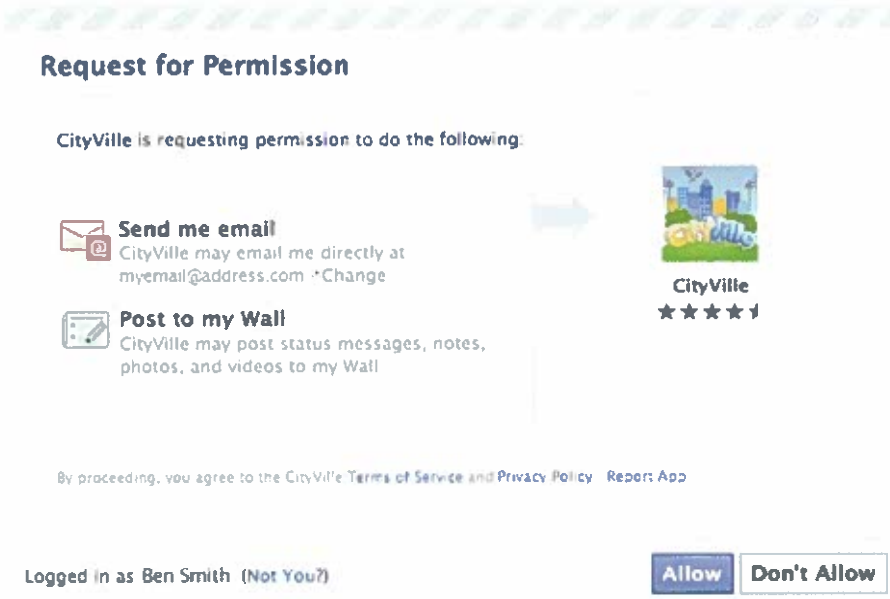
  - *Are teens sensitive users, warranting enhanced consent procedures?*

  - *Should additional protections be explored in the context of social media services? For example, one social media service has stated that it limits default settings such that teens are not allowed to share certain information with the category "Everyone." What are the benefits and drawbacks of such an approach?*

- *What choice mechanisms regarding the collection and use of consumer information should companies that do not directly interact with consumers provide?*

- *Is it feasible for data brokers to provide a standardized consumer choice mechanism and what would be the benefits of such a mechanism?*

Importance of choice. Facebook agrees that users should have the ability to make informed and meaningful choices about their online privacy. For example, in the case of third-party applications, we serve a dialog box that describes the categories of information that the application is requesting access to, and asks the user for his or her permission to proceed. The inclusion of granular information, in a context and at a time where users are likely to understand it, allows users to evaluate the application and decide whether they are comfortable authorizing it.



Implementing choice in different contexts. As the report recognizes, the ultimate goal is to offer users choice mechanisms that are easy to understand and easy to use. Because online services vary enormously and evolve quickly, static rules mandating the proper method for presenting choice are likely to prove counterproductive in the long run. For example, the report recommends that where user information will be conveyed to a third-party application developer, the notice-and-choice mechanism should appear "before the application obtains the consumer's information."[38] But such a rigid standard may actually hamper users' ability to make an informed decision. For instance, in a service that involves discrete transactions, it may be most effective to obtain a user's consent each time information about him is shared, while another service whose purpose is to provide a seamless experience should be permitted to obtain a user's consent in advance of any sharing to avoid the need to interrupt the user repeatedly with invasive disclosures and consent requests. In general, consent mechanisms are more effective if they are context-appropriate—that is, if they are designed in a way that reflects the nature of information being shared and maximizes the user's understanding of the service.

Enhanced choice for sensitive data. The staff recommends that affirmative express consent be required before children's, financial, medical, or precise geolocation data is collected, used, or shared. Facebook agrees that sensitive information may warrant enhanced consent. However, it is important to recognize that enhanced consent may not be possible in every instance. For example, a user might post a status update that referred to an illness or other medical condition, but it would be difficult for Facebook to know on an automated basis that the status update related to a "sensitive" category of information.

In cases like these, it would be inappropriate to charge service providers with the knowledge that they are receiving sensitive data or to impose a heightened notice-and-consent obligation upon them. In practice, large service providers like Facebook simply do not have the ability to review submissions by hand when they are received, meaning that a rigid rule imposing heightened obligations for sensitive

[38] FTC Report 59.

data would effectively preclude the collection of any data at all from users—stifling the very act of sharing on which the social web is based.

Special considerations for children. As the report accurately notes, "teens are heavy users of digital technology and new media but may not always think clearly about the consequences of their actions."[39] For this reason, we have special protections in place for minors, and we place restrictions on the ability of adults to share and connect with minors. One example of an enhanced consent procedure employed by Facebook is what we call social verification. Minors who are new to our service are asked to consider the source of a new friend request before they are able to confirm that they want to accept that request. Typical representative questions asked of the minor include the following: (i) Is this someone whom you know from your school?; or (ii) Is this someone whom you or your parents know from your community? In addition, while users over 18 on Facebook can share information with everyone, users under 18 are automatically restricted to sharing with a much smaller subset of users, such as the minor's friends, friends of those friends, and their verified networks, generally associated with their schools. Although we recognize that these mechanisms have the potential to provide minors with a more limited Facebook experience, we believe that such restrictions are necessary to ensure that minors connect with other users in safe and age-appropriate ways.

Choice: Do Not Track mechanism for online behavioral advertising

- *How should a universal choice mechanism be designed for consumers to control online behavioral advertising?*
- *How can such a mechanism be offered to consumers and publicized?*
- *How can such a mechanism be designed to be clear, easy-to-find, usable, and understandable to consumers?*
- *How can such a mechanism be designed so that it is clear to consumers what they are choosing and what the limitations of the choice are?*
- *What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?*
- *How many consumers would likely choose to avoid receiving targeted advertising?*
- *How many consumers, on an absolute and percentage basis, have utilized the opt-out tools currently provided?*
- *What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?*
- *In addition to providing the option to opt out of receiving ads completely, should a universal choice mechanism for online behavioral advertising include an option that allows consumers more granular*

[39] FTC Report 62.

control over the types of advertising they want to receive and the type of data they are willing to have collected about them?

- *Should the concept of a universal choice mechanism be extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications?*

- *If the private sector does not implement an effective uniform choice mechanism voluntarily, should the FTC recommend legislation requiring such a mechanism?*

In recommending the creation of a Do Not Track mechanism for behavioral advertising, the staff report correctly recognizes that one of the primary privacy concerns associated with online behavioral advertising is that "[c]ompanies engaged in behavioral advertising may be invisible to most consumers."[40] Because many of the companies that use invisible web beacons, cookies, or other technologies to collect information for ad targeting purposes do not have direct relationships with users, users have few ways of identifying which companies are tracking them, few ways of expressing their privacy preferences, and few ways of holding companies accountable for their privacy practices.

The same concerns are not implicated when the user has a relationship with the company conducting the tracking and understands that the entity may be collecting data. For example, Facebook's social plugin enables users to go the *Washington Post* website and see a list of news stories that their Facebook friends have found interesting. The social plugin also makes it easy for users to recommend news stories, fostering the kind of interactive discussion and community engagement that is a hallmark of the social web. Although the social plugin collects information so that it knows which *Washington Post* news articles the user has shared or commented on, this kind of tracking is a far cry from the covert surveillance that users are most worried about. Facebook's presence on the *Washington Post* website is clear, meaning that Facebook users know who is collecting the information and have various means of communicating with Facebook if they are concerned about Facebook's information practices.

As noted above, there are other situations in which the FTC has adopted a contextual approach that takes into account the differences in user expectations. For example, the popular Do Not Call program contains an exception for established business relationships. Under the FTC's telemarketing sales rule, an entity can make calls to a telephone number listed on the national "Do Not Call" registry if it has an established business relationship with the call recipient.[41] This exception is consistent with people's expectations: although people may not want to receive unsolicited telemarketing generally, they are less likely to object to such calls when they have recently purchased or made inquiries about a product that the caller is selling.[42] The Do Not Call registry helps people convey their privacy preferences to the telemarketing industry at large, but people who receive telemarketing calls from entities with whom they have an established business relationship have other means of controlling the entity's information

---

[40] FTC Report 63.

[41] 16 C.F.R. § 310.4(b)(1)(iii)(B)(ii).

[42] *See* 16 C.F.R. § 310.2(n) (defining established business relationship to mean a relationship based on a financial transaction between the consumer and the seller within the 18 months preceding the call, or an inquiry by the consumer within the 3 months preceding the call).

practices. For example, they can request that the entity stop calling them,[43] terminate the relationship, or engage in grassroots public relations efforts to attract regulatory or market scrutiny of the entity's conduct.

Given the speed at which the online advertising industry is evolving, Facebook believes that legislation imposing a Do Not Track mechanism would be premature. There are already numerous private-sector initiatives under way to address users' concerns about behavioral advertising. The Digital Advertising Alliance has been working to develop and implement self-regulatory principles since 2009, and enforcement mechanisms are coming into effect this year. Within days of the release of the FTC's report, a group of data brokers announced the formation of the Open Data Partnership, which permits users to view and edit the information that has been collected about them. Three leading browser manufacturers also announced that they are developing powerful tools that will allow users to exercise persistent control over third-party tracking.[44] Facebook believes that the private sector can and will persevere in developing creative solutions that protect personal information while preserving the vitality of the digital economy. Any legislative or regulatory attempt to mandate a particular technological fix might become outdated as technology and user expectations continue to evolve.

Finally, Facebook notes that the staff report appropriately focuses on the use of data for online behavioral advertising, as opposed to any and all tracking. As discussed in our overview letter, companies engage in various forms of monitoring in order to protect user security, ensure the effectiveness of their services, and find new ways of responding to user needs. These kinds of data collection have been inherent in the structure of the Internet since its inception and, as the staff acknowledges, users generally accept that they do not raise the same issues as tracking for the purpose of behavioral targeting.

Transparency: Improved privacy notices

- *What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?*

- *How can companies present these notices effectively in the offline world or on mobile and similar devices?*

- *Should companies increase their use of machine-readable policies to allow consumers to more easily compare privacy practices across companies?*

Facebook agrees with the staff's suggestion that clearer, shorter, and more standardized privacy notices would help users understand and compare companies' privacy practices. Facebook also welcomes the

---

[43] *See* 16 C.F.R. § 310.4(b)(1)(iii)(A).

[44] In his concurrence, Commissioner Kovacic asks how a Do-Not-Track mechanism that merely conveys consumers' request not to be tracked can be enforced. *See* FTC Report D-3. The various private-sector initiatives discussed in this paragraph indicate that industry is already taking steps to help users communicate their privacy preferences and to ensure that companies honor those preferences, even in the absence of a legal requirement to do so.

report's recognition that any attempt to standardize privacy notices across industries will be a formidable challenge in light of ongoing changes in technology.[45] Because a rigid "check box" approach that purports to cover all online actors might unduly limit companies' ability to fully describe their data practices, Facebook suggests exploring the possibility of sector-specific privacy notices. As discussed in the overview letter, Facebook believes that transparency could be promoted by allowing each industry sector to develop a common privacy notice describing the data-handling processes in that particular sector, which would then be supplemented by individual companies' descriptions of their own unique practices. This approach would allow companies to provide more detail about their data-handling procedures without lengthening their privacy policies, while also allowing users to identify any salient differences between companies.

The report also requests input on how companies can more effectively present privacy notices on mobile devices. Although designing effective ways to display information on mobile phones and other devices with limited interface options is a continuing challenge for industry, at Facebook we believe that individuals should be empowered with the information they need to make effective privacy decisions regardless of what platform or device they use. Most of the privacy settings available on the Facebook.com site also can be accessed and changed by users who connect to Facebook through mobile devices, and these preferences are effective when mobile users access Facebook through other platforms, including our Facebook.com website. This enables our users to make consistent, real-time decisions about the data they share—no matter where they are or what devices they prefer to use when connecting with their friends and communities. We expect that industry will continue to create innovative solutions to the problem of presenting effective privacy notices on mobile devices.

Transparency: Reasonable access to consumer data

- *Should companies be able to charge a reasonable cost for certain types of access?*
- *Should companies inform consumers of the identity of those with whom the company has shared data about the consumer, as well as the source of the data?*
- *Where companies do provide access, how should access apply to information maintained about teens? Should parents be able to access such data?*
- *Should access to data differ for consumer-facing and non-consumer-facing entities?*
- *For non-consumer-facing companies, how can consumers best discover which entities possess information about them and how to seek access to their data?*
- *Is it feasible for industry to develop a standardized means for providing consumer access to data maintained by non-consumer-facing entities?*

---

[45] *See* FTC Report 72 (requesting comments on "the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology").

- *Should consumers receive notice when data about them has been used to deny them benefits? How should such notice be provided? What are the costs and benefits of providing such notice?*

In recommending that companies provide reasonable access to data, the report notes that there are important distinctions between consumer-facing companies and those whose collection activities are largely invisible to the public. Facebook appreciates the staff's attention to this crucial point. As discussed elsewhere in these comments, when users understand which company is collecting information about them, users have many avenues by which they can express their concerns about the company's information practices. Fewer tools are available to users with respect to businesses that collect and use information without the user's knowledge. Access becomes correspondingly more important as a method for ensuring that these non-consumer-facing companies take reasonable steps to safeguard user privacy.

Transparency: Material changes

- *What types of changes do companies make to their policies and practices and what types of changes do they regard as material?*

- *What is the appropriate level of transparency and consent for prospective changes to data-handling practices?*

Facebook, like most other online service providers, is constantly striving to build new features and products that will enrich users' online interactions. Sometimes these innovations require changes in our data-handling practices.

Consistent with our commitment to providing clear and transparent policies, we believe that users should be informed whenever a company significantly changes its procedures. Indeed, we have taken the extra step—one that is virtually unique in the industry—of allowing users to vote on proposed changes to our privacy policy if comments reach a certain threshold. We also believe that companies should tell users in advance how such notifications will be provided—e.g., on a standard place on the company's website. As discussed in our overview letter, however, any notice or consent requirements for material changes must be sensitive to factors such as the nature of the user's relationship with the business, whether the user will be surprised by the change, and whether the change will add value that the user appreciates. In some situations, as the staff report recognizes, a confusing opt-in may be a less meaningful way of protecting privacy than a process that provides users with advance notification of the proposed change and gives them adequate time to opt out, adjust the amount of information that they choose to share, or close their accounts entirely before the change takes effect.

Transparency: Consumer education

- *How can individual businesses, industry associations, consumer groups, and government do a better job of informing consumers about privacy?*

- *What role should government and industry associations have in educating businesses?*

Facebook agrees that educational initiatives are needed to improve user awareness of privacy issues. Although all stakeholders have a part to play in increasing user understanding, businesses occupy a unique position from which to raise awareness because they typically have the most extensive

interactions with users. For example, when we introduced our Privacy Transition Tool in December 2009, every user, worldwide, was required to stop and consider his or her privacy settings before using the service further. Hundreds of millions of individuals took time to meaningfully consider the nature of privacy on the social web. Similar tools can offer users insight into the privacy implications of their Internet activity, enabling users to make informed decisions that accurately reflect their individual preferences.

While industry can and should use its relationship with users to increase users' understanding of privacy issues, the government also should take steps to educate the public on privacy and to encourage the development of industry-specific campaigns to provide users with privacy suggestions. Ultimately, the goal of these education efforts should be to inform users adequately about the benefits, risks, and options inherent in sharing information about themselves. In combination with efforts to provide users with context-sensitive control, education programs will empower users to make the choices that are right for them.