January 28, 2011

VIA ELECTRONIC DELIVERY

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

Re: Commercial Data Privacy and Innovation in the Internet Economy:
A Dynamic Policy Framework
Docket No. 101214614–0614–01

Dear Internet Policy Task Force:

Facebook appreciates the opportunity to comment on the Department of Commerce's proposed privacy framework for businesses and policymakers. This framework, together with the privacy framework proposed by the Federal Trade Commission, 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 Department and the FTC 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 Department has acknowledged, 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 Department'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 Department has expressly emphasized the importance of updating our nation's privacy framework to reflect "the digital economy's complexity and dynamism" in

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

a way that will "allow innovation to flourish while building trust and protecting a broad array of other rights and interests."[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 Department and FTC 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] 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) [hereinafter Commerce Report]; *see also* 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) (agreeing that a new framework should "tak[e] a flexible and evolving approach to privacy protection, designed to keep pace with a dynamic marketplace") [hereinafter FTC 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 Department of Commerce and FTC 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 Department's 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 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 with the friends and people around them, 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 social web also 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 demonstrations against the FARC terrorist group in

---

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

2008.[4] The Berkman Center for Internet and Society at Harvard University cited Facebook and Twitter as playing key roles in spreading dissent—and up-to-the-minute news—in Tunisia, leading to the removal of Zine El Abidine Ben Ali, who gained control of the country in a 1987 coup d'état.[5]

Quite apart from these highly visible Facebook and Twitter "revolutions," 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 FTC 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."

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

---

[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).

[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").

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 balance our users' desire to express themselves against 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

Both reports recommend that companies consider privacy issues systematically, building robust privacy protections into the design process and throughout their organizations. The Commission 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]

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

---

[9] Commerce Report 47.

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

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 help users take charge of their privacy decisions.

- 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 of 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.

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 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. 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.** 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.

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.

III. INDIVIDUAL EMPOWERMENT AND RESPONSIBILITY

Facebook agrees with the Commerce Department and the FTC 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 Commerce's suggestion that information about data practices "must be accessible, clear, meaningful, salient, and comprehensible to its intended audience,"[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

---

[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.

[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] Commerce Report 31.

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'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 FTC recommends that companies obtain affirmative consent from users before using previously collected data in a "materially different manner" than described in an earlier 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 FTC observes, "a clear, simple, and prominent opt-out mechanism may be more privacy protective than a confusing, opaque opt-in."[16] The FTC also endorses in some situations the use of "a 'just-in-time' approach, in which the

---

[15] FTC Report 77.

[16] FTC Report 60.

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 Commerce report notes,[20] it is important to consider whether the change is likely to bring social benefits that users want. 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

---

[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.

[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.

changes in users' expectations. For example, the FTC proposes that "just in time" notice should not be required when an entity collects information for what the FTC calls a "commonly accepted practice."[22] Facebook agrees that notice would be inappropriate and deemed intrusive when the disclosures that would be provided 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.

One promising option for implementing choice may be the adoption of "do not track" functionality, which the FTC 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 Commission'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 with the government if they object to an approach taken by a company they know: they can complain about that company by name to Congress or the FTC or force a reduction in that company's stock price through grassroots public relations efforts. None of these corrective

---

[22] FTC Report 53–55.

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]

IV. INDUSTRY ACCOUNTABILITY

In their reports, the FTC and Commerce 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.

---

[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).

[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.

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 Firefox, and Google Chrome—have announced functionality that responds to the FTC'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. 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

---

[26] 15 U.S.C. § 45(n).

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]

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 Commerce Department and the Commission 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 Commerce Department's observation that any privacy framework must be *dynamic*. By implementing the principles in a way that accommodates the evolving

---

[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 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.

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.

Enclosure

JANUARY 28, 2011

RESPONSES TO DEPARTMENT OF COMMERCE QUESTIONS

"COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK"

Facebook appreciates the opportunity to submit these responses to the recommendations and questions that the Department of Commerce's Internet Policy Task Force raises in its report proposing a new dynamic policy framework for protecting privacy and innovation. To facilitate review, our responses address many of the questions raised by the Department and follow the same order as the topics addressed on pages 23 through 67 of the report.

Implementation of Fair Information Practice Principles ("FIPPs")

1. The Task Force recommends adoption of a baseline commercial data privacy framework built on an expanded set of Fair Information Practice Principles (FIPPs).

- *Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or through other formal means to address how current privacy law is enforced?*

- *How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement actions?*

- *As policymakers consider baseline commercial data privacy legislation, should they seek to grant the FTC the authority to issue more detailed rules? What criteria are useful for deciding which FIPPs require further specification through rulemaking under the Administrative Procedure Act?*

- *Should baseline commercial data privacy legislation include a private right of action?*

Facebook agrees that implementation of FIPPs could help elevate "substantive privacy protection [over] procedural hurdles," encouraging companies to better serve users by providing more transparency and tools for controlling personal data.[1] However, the task of providing substantive meaning to these privacy principles is best accomplished by allowing each industry sector to compete on privacy issues and to engage in self-regulation. Industry self-regulatory efforts are more nimble, more nuanced, and better able to respond to evolving technologies and user expectations than cumbersome legislation or regulation.

It is unlikely that any attempt to elaborate on FIPPs through statutes or agency rules will be agile enough to account for the speed of innovations in Internet services and technology. As the Department recognizes, the rulemaking process "can take years and often results in rules addressing services that

---

[1] Commerce Report 4.

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

may be long abandoned."[2] In contrast, as discussed below, industry self-regulatory approaches can be flexible enough to keep up with technological and economic growth but concrete enough to provide important privacy protections to users. They also can themselves contain enforcement mechanisms that can be supported by Federal Trade Commission enforcement action where appropriate.

Enhancing Transparency Through Better Privacy Disclosures

2. To meet the unique challenges of information intensive environments, FIPPs regarding enhancing transparency; encouraging greater detail in purpose specifications and use limitations; and fostering the development of verifiable evaluation and accountability should receive high priority.

- *What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.*

- *What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?*

As the Department notes, lengthy, complex, and unintelligible privacy notices provide little insight into companies' actual privacy practices and interfere with users' ability to make informed choices.[3] Complicated and formalistic privacy policies have proliferated in part because many companies feel the need to use them to manage the uncertainty associated with the possibility of FTC enforcement, private claims, and other liabilities. In essence, some companies' privacy policies function primarily as disclaimers rather than disclosures.

One way to address this concern is the Department's proposal that the government encourage the development of voluntary, enforceable privacy codes of conduct for individual industries. These codes of conduct could, among other features, include industry-wide model privacy policies that set forth the basic features of how participants in a particular industry use data that they collect about individuals. Companies could adopt these disclosures and provide concise explanations of how their own practices differ from the standard, making it easy to compare privacy practices across competitors. And companies could be encouraged to adopt these notices through the use of a safe harbor approach like the one proposed by the Department—what the report referred to as a "carrot" and "stick" approach—which would protect companies from liability if they provide disclosure in conformance with an industry code of conduct.[4]

The proposed Privacy Policy Office ("PPO") could serve as a useful forum for bringing companies and trade groups together to draft these common industry privacy notices. The PPO also could play a helpful

---

[2] Commerce Report 47.

[3] Commerce Report 31.

[4] Commerce Report 43.

role in assembling information and drawing attention to best practices, to spur sectors or companies that may be slower in developing their own privacy notices.

Facebook agrees, however, with the Department's conclusion that "[t]he range of services, business models, and organizational structures . . . counsel against attempting to develop comprehensive, prescriptive rules"[5] for enhancing transparency. The legislative and rulemaking process is slow, and any attempt to regulate across multiple sectors likely would result in rules that are too broad to provide meaningful guidance to companies as well as privacy notices that are too vague to provide helpful information to users.

Enhancing Transparency Through Privacy Impact Assessments ("PIAs")

- *What are the elements of a meaningful PIA in the commercial context? Who should define these elements?*

- *What processes and information would be useful to assess whether PIAs are effective in helping companies to identify, evaluate, and address commercial data privacy issues?*

- *Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?*

Facebook believes that companies should be encouraged to evaluate privacy issues in almost every division of the organization and at every stage of the product lifecycle. Such evaluations should include consideration of what information is being collected, what notices are given to the user, what choices the user has, who is authorized to access the information, what limitations are placed on third parties' access, what training is provided to employees, and whether there are appropriate internal review and approval procedures. Some elements will be more or less relevant depending on the context in which the company is collecting the information and the service or product being offered.

The Department also solicited input on whether there should be a requirement to publish PIAs in a standardized or machine-readable format. Given the wide variety of practices and the likelihood of changes to technology and Internet services after any disclosure standard is adopted, imposing a standardized format might undermine companies' ability to provide information about their specific data-handling procedures. PIAs might also contain competitively sensitive information that companies will hesitate to disclose. Companies therefore should be encouraged to publish PIAs as an additional or alternative means of enhancing transparency and providing insight into their privacy-related processes, but they should not be required to do so.

Other Methods of Enhancing Transparency

- *What are consumers' and companies' experiences with systems that display information about companies' privacy practices in contexts other than privacy policies?*

---

[5] Commerce Report 32.

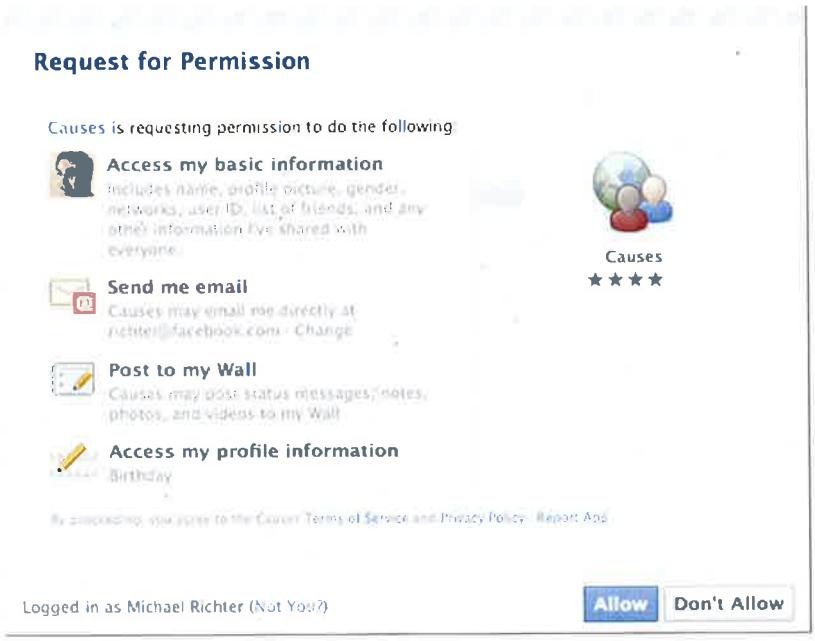
- *What are the relative advantages and disadvantages of different transparency-enhancing techniques in an online world that typically involves multiple sources being presented through a single user interface?*

- *Do these (dis)advantages change when one considers the increasing use of devices with more limited user interface options?*

The Department requested comments on mechanisms other than traditional privacy policies that could be used to describe privacy practices. Our experience has been that privacy disclosures are most effective when information is presented visually, such as through screenshots, videos, and interactive tools. Examples of interactive tools that we offer include the following: our privacy center, which allows users to adjust their individual settings; publisher privacy controls that allow users to choose their audience every time they post information; and our application dashboard, which allows users to manage the applications that have access to their information.

As the report recognizes, the rise of the social web means that the online experience today often involves multiple companies providing content and services through a single interface.[6] At Facebook, this arises in the context of third-party applications that use Facebook Platform and our social plugins.

In the case of third-party applications, we provide 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. 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.



[6] *See* Commerce Report 37.

Similarly, when we serve social plugins on third-party sites, we take steps to make sure that the user understands that they are interacting with Facebook. We also designed our social plugins such that we do not give user information to the third party sites.

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 users access Facebook through other platforms, such as 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.

Purpose Specifications and Use Limitations

- *Are purpose specifications a necessary or important method for protecting commercial privacy?*
- *Currently, how common are purpose specification clauses in commercial privacy policies?*
- *Do industry best practices concerning purpose specification and use limitations exist? If not, how could their development be encouraged?*
- *What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?*
- *How should purpose specifications be implemented and enforced?*
- *How can purpose specifications and use limitations be changed to meet changing circumstances?*

The report acknowledges that purpose specifications and use limitations sometimes must be changed to meet changing circumstances,[7] and Facebook appreciates the Department's attention to this crucial point. As noted above, an overly restrictive legal regime that prevents companies from changing their data-handling practices to incorporate beneficial new features does not serve the interests of users or existing businesses. Such a regime would result in legalistic, "laundry list" style disclosures that preserve rights for service providers but do not offer users accessible information about how a company will use the data that it collects. Companies need the flexibility to adjust their uses of information over time. Indeed, 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.

Consistent with Facebook's commitment to providing clear and transparent policies, we believe that users should be informed whenever a company significantly changes its information practices and that

---

[7] Commerce Report 38–40.

companies should establish predictable ways for communicating changes to individuals. However, as discussed in our overview letter, the appropriate level of consent should be calibrated according to context-sensitive factors such as the nature of the individual's relationship with the company, whether the individual will be surprised by the change, and whether the change will add value that the individual appreciates. Requiring companies to obtain consent for every change often is unnecessary given the nature of the relationship between most users and their online service providers, and such a requirement—because it might be impossible to obtain consent from every single user—could effectively preclude companies from making any improvement to the products and services that they offer.

Evaluation and Accountability

- *Who should be responsible for demonstrating that a private sector organization's data use is consistent with its obligations? What steps should be taken if inconsistencies are found?*
- *Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?*
- *Are technologies available to help companies monitor their data use, to support internal accountability mechanisms?*
- *How should performance against stated policies and practices be assessed?*
- *What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purposes and use limitations*?

Facebook agrees with the Department's observations about the importance of accountability, and we believe that there are many methods to ensure that organizations offer effective protections and maintain user trust. As described elsewhere in these comments, accountability can be achieved through a combination of voluntary industry codes of conduct, safe harbor protection for entities that comply with a code of conduct, FTC enforcement for unfair and deceptive privacy practices, and transparency-based market mechanisms (such as the threat of user defection for companies that materially violate their privacy commitments).

Development of Voluntary Codes of Conduct

3. Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs. To encourage the development of such codes, the Administration should consider a variety of options, including (a) public statements of Administration support; (b) stepped up FTC enforcement; and (c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multistakeholder processes.

Facebook supports the Department's suggestion that voluntary codes of conduct can bridge the gap between general FIPPs and specific guidance on how they should be implemented, including through the use of model privacy practice disclosures. Facebook agrees that the government can and should

encourage the development of these codes through public statements of support, convening stakeholders, and similar activities.

Facebook also agrees with the Department's suggestion that these codes of conduct could be made enforceable through the use of the safe harbor approach described above and in the Department's report, which would protect businesses that complied with a code of conduct from FTC enforcement.[8] In this regard, Facebook notes that additional legislation is not required to implement a safe harbor regime. Instead, since the FTC's enforcement authority in this area is derived from Section 5 of the FTC Act, which regulates unfair and deceptive trade practices, the FTC could announce its determination that compliance with certain voluntary industry codes was *per se* evidence that a company's privacy practices were not unfair or deceptive and that it would not take enforcement action against companies that complied with such a code. Of course, the FTC also could bring a deceptiveness action against a company that falsely asserted compliance with a voluntary industry code.

Establishment of Privacy Policy Office

4. Using existing resources, the Commerce Department should establish a Privacy Policy Office (PPO) to serve as a center of commercial data privacy expertise. The proposed PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together; and it would work in concert with the Executive Office of the President as the Administration's lead on international outreach on commercial data privacy policy. The PPO would be a peer of other Administration offices and components that have data privacy responsibilities; but, because the PPO would focus solely on commercial data privacy, its functions would not overlap with existing Administration offices. Nor would the PPO would have any enforcement authority.

- *Should the FTC be given rulemaking authority triggered by failure of a multi-stakeholder process to produce a voluntary enforceable code within a specified time period?*

- *How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?*

- *Under what circumstances should the PPO recommend to the Administration that new policies are needed to address failure by a multi-stakeholder process to produce an approved code of conduct?*

- *How can cooperation be fostered between the National Association of Attorneys General, or similar entities, and the PPO?*

Facebook supports the Department's efforts to create a Privacy Policy Office and believes that the proposed PPO could play a useful role in fostering multi-stakeholder discussions of implementation models, best practices, and collaborative solutions. As discussed above, we believe that the PPO could provide a valuable forum for the development of voluntary, sector-specific, enforceable codes of conduct that address emerging technologies and issues in a dynamic way.

---

[8] Commerce Report 43.

The Department also requested input on mechanisms that would encourage the development of voluntary codes of conduct, and the safe harbor discussed above is one such mechanism. But we believe that it would be premature to adopt rigid enforcement mechanisms, such as a specific deadline that would trigger FTC rulemaking authority. At present, the details of how the PPO will operate and the extent to which it will jumpstart the development of industry codes are still unknown. In addition, it is important to recognize that the time required to develop a given code of conduct will depend on the technical complexity of the issue, the number of actors in that sector, the degree of coordination required, and whether progress is being made on technological or other fronts that could potentially provide a different resolution to the problem. Instead of setting inflexible deadlines now, the Department first should allow industry to engage with the PPO, subject to the understanding that the Department may revisit the issue of enforcement mechanisms at a later date if insufficient progress is being made.

FTC Enforcement

5. The FTC should remain the lead consumer privacy enforcement agency for the U.S. Government.

- *Do FIPPs require further regulatory elaboration to enforce, or are they sufficient on their own?*
- *What should be the scope of FTC rulemaking authority?*
- *Should FIPPs be considered an independent basis for FTC enforcement, or should FTC privacy investigations still be conducted under Federal Trade Commission Act Section 5 "unfair and deceptive" jurisdiction, buttressed by the explicit articulation of the FIPPs?*
- *Should non-governmental entities supplement FTC enforcement of voluntary codes?*
- *At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval? Potential options include providing an ex ante "seal of approval," delaying approval until the code is in use for a specific amount of time, and delaying approval until enforcement action is taken against the code.*
- *What steps or conditions are necessary to make a company's commitment to follow a code of conduct enforceable?*

The FTC's Section 5 enforcement power over unfair and deceptive trade practices already gives it the ability to investigate violations of well-recognized FIPPs such as data security, as well as any misleading promises by companies to adhere to industry codes of conduct based on FIPPs. Nongovernmental trustmark and certification authorities, such as TRUSTe and the Council of Better Business Bureaus, also supplement FTC enforcement in valuable ways: they can mediate disputes, monitor companies' commitments to follow an industry code of conduct, and refer violations to the FTC for further review. Indeed, these organizations have consistently been able to resolve privacy disputes internally rather than referring them to the FTC in the context of the U.S. companies that participate in the U.S. Department of Commerce–European Commission Safe Harbor framework, suggesting that these private enforcement mechanisms have been both highly effective and more efficient than government enforcement.

Because the existing enforcement mechanisms are sufficient to protect individuals from concrete harms caused by companies' privacy practices, Congress and the FTC should refrain from undertaking further legislative or regulatory action that might impede companies' ability to build the kinds of innovative online services that users have come to expect and demand.

Global Interoperability

6. The U.S. government should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other countries' commercial data privacy frameworks. The United States should also continue to support the APEC Data Privacy Pathfinder project as a model for the kinds of principles that could be adopted by groups of countries with common values but sometimes diverging privacy legal frameworks.

Facebook welcomes the Department's ongoing efforts to develop a coherent international legal framework for commercial data privacy. Harmonization of the relevant data protection rules would assist Facebook in offering its service to its global user base and support the growth of creative new features that build connections and communities around the world.

National Security Breach Notification

7. Consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Such a framework should track the effective protections that have emerged from State security breach notification laws and policies.

- *What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?*

Facebook agrees with the Department's recommendation that consideration should be given to a national data security breach notification framework. A comprehensive, unified approach would provide baseline protections for users and assist companies who must currently monitor and comply with a shifting patchwork of state data breach notification laws. However, any national law must include a risk assessment based on the potential harm from the breach. If companies are required to notify users about every breach, even those where there is no chance of actual harm, users will likely be inundated by a flood of notices and may eventually begin to disregard the notices they receive. Notices that contain genuinely important and urgent information may get lost amid the background noise.

Sector-Specific Privacy Regulation

8. A baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans, but rather should act in concert with these protections.

- *Are there lessons from sector-specific commercial data privacy laws—their development, their contents, or their enforcement—that could inform general U.S. commercial data privacy policy?*

The U.S. experience with sector-specific laws highlights the value of focusing on context and how data is collected, used, and shared within a particular industry. For example, the model financial privacy notice developed in 2009 by a consortium of eight agencies was successful because many financial institutions engage in similar practices. But an attempt to standardize privacy policies across multiple sectors will likely prove less helpful for users, because companies' practices vary enormously and a standardized privacy policy would only be able to provide vague descriptions of the companies' widely divergent practices. A better solution, as described above, would be the development of common privacy notices, developed by industry groups and adopted voluntarily by companies, supplemented by company-specific descriptions to highlight differences from industry-standard practices.

Preemption of State Laws

9. Any new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.

- *Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving States free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?*

- *How could a preemption provision ensure that Federal law is no less protective than existing State laws? What are useful criteria for comparatively assessing how protective different laws are?*

- *To what extent should State Attorneys General be empowered to enforce national FIPPs-based commercial data privacy legislation?*

- *Should national FIPPs-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?*

For the reasons discussed above, Facebook believes that industry self-regulatory efforts are better suited to advancing the interests of privacy and continued innovation than national commercial data privacy legislation. If, however, Congress decides to act in an area affecting online privacy, it should include a preemption provision that appropriately balances states' interests in protecting their residents and the recognition that federal policy is in some cases a better tool for helping users understand and exercise the privacy controls that are available to them. Users are often unaware of the choices provided by state-specific privacy requirements such as California's "Shine the Light Law." Uniform federal standards, by contrast, are usually more broadly understood and therefore more effective as a means of safeguarding users' privacy interests.

At the same time, Facebook recognizes that states have and should continue to have a role in protecting privacy. Facebook believes that state attorneys general should be empowered to enforce fair and

uniform federal standards, and that the valuable protections provided by state unfair and deceptive trade practices statutes should be preserved.

Electronic Communications Privacy Act ("ECPA")

10. The Administration should review the Electronic Communications Privacy Act (ECPA), with a view to addressing privacy protection in cloud computing and location-based services. A goal of this effort should be to ensure that, as technology and market conditions change, ECPA continues to appropriately protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.

- *The Task Force seeks case studies and statistics that provide evidence of concern—or comments explaining why concerns are unwarranted—about cloud computing data privacy and security in the commercial context. We also seek data that link any such concerns to decisions to adopt, or refrain from adopting, cloud computing services.*

- *The Task Force also seeks input on whether the current legal protections for transactional information and location information raise questions about what privacy expectations are reasonable and whether additional protections should be mandated by law. The Task Force also invites comments that discuss whether privacy protections for access to location information need clarification in order to facilitate the development, deployment and widespread adoption of new location-based services.*

Facebook agrees that the ECPA standards need to be revised in a way that provides stronger privacy protections for communications and associated data while accounting for changes in technology and usage patterns. The current legal landscape leaves companies uncertain about their compliance obligations, leaves law enforcement officials uncertain about their ability to obtain information needed in the course of their investigations, and leaves users uncertain about the privacy protections afforded to the communications they make online. For example, Facebook recently has received conflicting judicial decisions concerning civil litigants' ability to access communications made by users on Facebook, making it difficult for us to predict our obligations. Updated ECPA rules would help safeguard privacy and provide clarity to individuals, industry, and government alike.