facebook

December 21, 2011

The Honorable Joe Barton
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6155

The Honorable Edward J. Markey
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, DC 20515-6155

Dear Congressmen Barton and Markey:

This letter responds to your inquiry regarding Facebook's February 8, 2011 patent application and recent statements about information transmitted to Facebook when people visit third-party websites that have chosen to incorporate Facebook functionality. We appreciate the opportunity to respond to your questions.

We first want to emphasize that regardless of where people use Facebook, we are strongly committed to maintaining their trust regarding the collection, use, and disclosure of their information. These commitments are evidenced in the audit report released today by the Office of the Data Protection Commissioner of Ireland.[1] Ireland is the headquarters for Facebook in Europe and this audit by the Irish Data Protection Commissioner provides the most substantial and broad-based analysis of Facebook's current practices and policies to date. Although the Irish Data Protection Commission does not have jurisdiction over Facebook's activities in the United States, the practices and policies that it audited are the same as those in effect at Facebook in the United States. Relevant to your letter, the Data Protection Commissioner reviewed our use of information transmitted to Facebook when people visit third-party websites that have chosen to incorporate Facebook functionality and, as we explain further below, concluded that Facebook, does not use that information to build profiles of people based on their web-surfing or to target advertising. More generally, as part of the Irish audit, Facebook has agreed either to implement, or to consider further, specific best practices recommended by the audit team, the vast majority of which also will apply to our practices in the United States.

The commitments we have made as part of our audit by the Irish Data Protection Commissioner build upon our agreement with the Federal Trade Commission to formalize and enhance our privacy program. The comprehensive program that we are developing will address

[1] Facebook Ireland, Ltd., Report of Audit of Irish Data Protection Commissioner (*available at* http://dataprotection.ie/viewdoc.asp?DocID=1182&m=f).

the privacy risks related to new and existing services and ensure that appropriate privacy and security protections are integrated into those services. It also will be evaluated by an independent outside auditor, who will be responsible for assessing whether we are meeting our obligations over the next twenty years.

As the Irish Data Protection Commissioner's audit report and our agreement with the FTC demonstrate, Facebook is committed to working with regulators, advocates and experts to inform our data practices and policies. The commitments will ensure people's Facebook experience on third-party websites—now and in the future—is consistent with our commitments to protecting privacy.

With this background in mind, we address each of your questions in turn.

1. What is the purpose of the filed patent and how does Facebook intend to use it?

The purpose of the filed patent is to protect our intellectual property developed by engineers who are constantly innovating and developing new technologies and ideas, which can be used in many different ways. When we develop these new technologies and ideas, we want to use the legal tools available to us, including patents, to protect them. As a result, we sometimes file patent applications or take other legal steps to protect our intellectual property even if we don't intend to use our ideas in our products.

The practice of obtaining patents on inventions without launching products based on them is common in the technology industry, and no conclusions should be drawn about a company's practices, products or services from the patents it files, acquires or holds in its portfolio. While it is commonplace for established technology companies to build large patent portfolios, a substantial number of the patents that make up those portfolios are never commercialized or implemented in product offerings. In fact, by some estimates, more than half the patents issued the United States have never been commercialized.[2] It is very common for a company to file for, acquire and hold patents, despite the fact that it does not do, or intend to do, what is described in those patents. Indeed, there are entire businesses built on holding patents that do not produce a single product.

We discuss in detail in the answer to Question 2 the information we receive and record when people interact with pages that include Facebook functionality and how we use such information.

2. Is it the intention of Facebook to track users on other websites regardless of login status? What actions is Facebook currently taking to ensure that its users are not tracked when they visit other websites?

Unlike many other web-based companies, Facebook has not designed its advertising system to "track" people on third-party websites for the purpose of profiling their activities and

[2] *See* Ted Sichelman, *Commercializing Patents*, 62 Stan. L. Rev. pp. 341, 343, 363-66 (2010).

serving them targeted advertisements based on that activity. As the Irish Data Protection Commissioner found in its report released today:

> "As indicated elsewhere in this report, this Office conducted a thorough analysis of the use of information gathered from external websites via the social plug-in. This Office is satisfied (for the reasons stated elsewhere) that such information is not associated with the user or used in any way to build a profile of that user. Neither is there any profile formed of non-users which could be attributed to a person on becoming a user."[3]

> "We found no evidence, from a very extensive examination of code, logging and queries served to the logged data that the information gathered was used for any advertising, predictive or user profiling purposes."[4]

The Data Protection Commissioner rendered these findings only after performing tests of our use of the data collected through social plugins.[5] We provide background on social plugins and more detail on their integration into third-party sites below.

Background

Facebook allows third-party websites to display certain functionality of the Facebook website on their sites through social plugins, such as the "Like" button.[6] This allows the third-party website to present relevant information to a logged in Facebook user and to enable Facebook users to share content from that third-party site with their friends. This extends the experience of Facebook to other websites by enabling people to connect with friends and to recommend, comment on, and share content across the Internet.

As we have noted in the past and in our Data Use Policy, when a third-party website chooses to use Facebook features on their sites, Facebook records certain browser-related data when people visit those sites. The amount of data that a person's browser sends to Facebook depends on whether the person has visited Facebook in the past and whether the person is logged into Facebook when he or she visits the site. When a person who has never visited Facebook.com before visits a website with a social plugin, Facebook will receive and record through social plugins a limited list of standard browser information, including: (i) the website being visited, (ii) the date and time, (iii) the IP address of the computer, and (iv) information about the browser type and operating system. The transmission of this information is part of the

---

[3] *See* Report of Audit of Irish Data Protection Commissioner, p. 65.

[4] *See id.*, p. 74.

[5] *See id.*, p. 82 ("Tests were also performed to attempt to establish whether or not the act of a logged-in Facebook user simply browsing to pages that have social plugins (as opposed to clicking the "Like" button) would influence the advertising that the user is presented with. An affirmative result would strongly indicate that Facebook were using browsing activity to target advertising, which it is claimed is not the case. No correlation with browsing activity was identified.")

[6] For more information on our social plugins, *see* https://developers.facebook.com/docs/reference/plugins.

normal operation of the Internet: the information is sent to Facebook so that its servers can communicate with the person's browser and load the Facebook functionality onto the webpage.

In addition to this technical information, if the person has visited Facebook.com in the past, Facebook will record information that has been stored in a "cookie" that was previously set when the person visited our site. For people who have visited Facebook.com using their browser, we place a cookie on their browser that identifies the individual browser but does not include personally identifying information, such as name or contact information. This browser-identifying cookie helps us keep Facebook and the people who use it safe. For example, we want to know if the same browser is attempting to visit Facebook thousands of times in just a few seconds as part of a coordinated denial of service attack. Cookies help us prevent such attacks, and the more coverage of browsers visiting Facebook, the more effective this security feature is at protecting the people that use Facebook.

When a person is logged into Facebook and then visits a third-party site with a social plugin, the amount of information we record differs as needed to provide the personalized, social experience that people request when they login to Facebook. Specifically, when a person is logged into Facebook, we would use a cookie to confirm that the person is logged into a specific Facebook account so that we can customize the content presented through the social plugin with information about a person's friends and ensure that when someone clicks the "Like" button, the "Liked" information is associated with the right account.

Importantly, Facebook specifically designed its social plugins so as not to share information that people provide on Facebook with third-party sites. To do this, the social plugin pulls content directly from Facebook's website and sends it to the person's browser, allowing, in effect, a part of Facebook to appear on a non-Facebook site. As the Irish Data Protection Commissioner found in its report:

> "We have confirmed that the content of the social plugin iframe is delivered directly to the web browser from Facebook and the website on which the social plugin is hosted has no visibility of the content of the social plugin delivered."[7]

In short, Facebook's social plugin technology brings socially relevant content to users as they interact with other sites around the Internet without sharing any of that information with the hosting site.

Facebook also allows people to bring their information to the applications and websites that they use, while on Facebook or while visiting a third-party site. For example, when a Facebook user visits a third-party site, they may be able to log in or register with their Facebook account. By doing so, the user will be promoted by a Facebook permission screen that explains that information will be shared with the third-party site. And, after the user has authorized the application or website they are using to share information, they may use their Facebook settings to cancel that permission. This consent model allows people to experience third-party applications and websites in a way that protects their privacy.

---

[7] *See* Report of Irish Data Protection Commissioner, p. 80.

Data Practices Regarding Facebook Functionality On Third Party Sites

As described in detail above and as confirmed by the Irish Data Protection Commissioner, we have not designed our social plugins in order to "track" a person's activities across the websites he or she may visit to build a profile and target advertisements based on that information. The information that we record through social plugins is used to prevent unauthorized access to our services, deliver our services, and analyze internally how Facebook is being used across the Internet. Like other companies, we also may use the information we collect for internal operations, including data analysis, research, development, and service improvement.

Aside from social plugins, another instance in which we may receive information about people's visits to third-party sites is as necessary to measure click-through results from ads served on Facebook.com. In this context, we measure when and how frequently people click on the ads we display on our site and may record whether a person who clicked through an ad served on Facebook.com later purchased a product on the advertiser's site. This helps us give feedback to our advertisers about how effective their ads are and what ads people on Facebook find most relevant. This kind of analysis is similar to the analytics performed by other companies that display ads on the web. It is important to note that we do not use the information we record in this context to build a profile of people's online activities across third-party sites for the purpose of targeting advertisements to them based on that information.

Our longstanding explanation that we do not "track" people on third-party sites is consistent with the distinction made by the Federal Trade Commission in the preliminary staff report on consumer privacy that it issued last year. In this report, the staff suggested the implementation of a "Do Not Track" mechanism that would give people the choice to opt out of the collection of their information for online behavioral advertising purposes. The staff described this activity as "tracking." At the same time, it also noted that information may be collected on the Internet for a variety of other reasons—such as providing the services that people have requested—and suggested that, in its view, that activity would not constitute "tracking."[8]

In this regard, the staff report suggested that the definition of "tracking" should depend on the nature of a particular transaction where information is collected and the relationship between the consumer and the entity collecting the information. Thus, certain "commonly accepted practices" involving information collection that were obvious from the context of a transaction (e.g., collection to provide a product or service) or otherwise generally accepted (e.g., collection for fraud prevention or for "first-party" marketing) would not be considered "tracking." In contrast, the staff suggested that collection of information by entities that are "invisible to most users" for the purpose of ad targeting would be considered "tracking."[9]

---

[8] Fed. Trade Comm'n, Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* pp. 53-57, 63-69 (Dec. 1, 2010).

[9] *See id.*, pp. 53-56.

In the comments we submitted to the FTC staff on its report, we agreed with the FTC's contextual approach to defining "tracking." As we noted, information collection by a company whose presence on a particular webpage is clear does not present the same privacy concerns as the surreptitious behavioral tracking that is the focus of the FTC's Do Not Track proposal. When a person knows the identities of the parties with whom he or she is communicating on a particular webpage, the person can more easily learn about those parties' data practices, provide feedback, or even complain about the company to Congress or the FTC. In addition, when the person has an established relationship with one or more of those parties, that relationship reflects a degree of trust and gives the company a further incentive to use data in a way that is consistent with the person's expectations. And, when the company offers a service on the third-party website and a person affirmatively engages with the company on that site, the person's expectations around the collection and use of that information by the company meaningfully change.

Facebook continues to support this contextual approach and our recent statements about our data collection practices reflect this support.

3. How does Facebook intend to integrate the location data of its users into its targeted advertising system?

Our Data Use Policy describes the information about people's location that we collect and use for advertising purposes.[10] When an advertiser wishes to run an ad on Facebook.com, we give the advertiser the opportunity to choose a particular audience based on information that Facebook has received about location, such as when people identify themselves as living in a specific city, check into a particular place, or specify a location in a status update. For example, if a Washington, D.C. restaurant wanted to advertise only to people who have indicated on Facebook.com that they live in or are visiting Washington, Maryland, and Virginia, Facebook can select people who meet that criterion and serve the advertisement to them (without, of course, identifying the specific names of the people to the advertiser). In other words, an advertiser provides the parameters of the audience the advertiser would like to reach, and Facebook serves the advertisement to users who fall within those parameters.

* * *

Thank you for your letter. If we can provide any additional information, please do not hesitate to contact us.

Sincerely,

Erin M. Egan
Chief Privacy Officer, Policy
Facebook

[10] Our Data Use Policy can be found here: https://www.facebook.com/full_data_use_policy.