



May 27, 2011

The Honorable Edward J. Markey
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

The Honorable Joe Barton
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: Your letter of May 11, 2011

Dear Congressmen Markey and Barton:

Thank you for your letter regarding a May 10, 2011, blog post by a Symantec researcher, as well as a *Wall Street Journal* article that reported on that blog post. In the blog post, the Symantec researcher reported that some third-party applications that had integrated with the Facebook Platform could inadvertently expose “access tokens”¹ to third parties when Facebook users used the applications. Symantec first contacted us about this issue in mid-April, and, as with all reports of potential security vulnerabilities, we took Symantec’s report very seriously. Indeed, the Symantec researcher who wrote the blog post observed that Facebook took “corrective action to eliminate th[e] risk” *before* Symantec released its blog post, and emphasized that “to [Symantec’s] knowledge, no Facebook users were impacted by this issue.”² We appreciate this opportunity to provide additional information about the issue and Facebook’s response to it.

To understand Symantec’s report, it is important to first understand the Facebook Platform. Unlike other popular platforms, the Facebook Platform is not an operating system, and it does not execute computer code provided by developers. Rather, it is a set of tools that enable independent developers to make their own applications and websites personalized and social, by allowing them to obtain and use, with clear user consent, information of Facebook users. To date, hundreds of thousands of developers have used the Facebook Platform to develop millions of applications that, with user consent, provide innovative new social services to people who use Facebook. To illustrate, the Birthday Calendar application allows individuals to track Friends’ birthdays, anniversaries, and

¹ An access token is a sequence of numbers, letters, and symbols provided by Facebook to a developer to enable the developer to obtain data from Facebook that the user has authorized the developer to obtain or to perform actions authorized by the user, such as posting to the user’s Facebook Wall.

² <http://www.symantec.com/connect/blogs/facebook-applications-accidentally-leaking-access-third-parties?API1=100&API2=4165004>.

other important dates. Another application, named We Read, enables people to share book titles and book reviews with their friends. On the charitable front, the Causes application provides an online platform for individuals and organizations to raise funds for charitable causes. Countless other examples are providing hundreds of millions of users new and innovative social experiences every day.

Through the Facebook Platform, Facebook provides developers with access to a set of application programming interfaces, or APIs, that allow an application or website—once it has obtained a user’s permission through a standardized screen that identifies what information the application seeks to obtain—to access user information in accordance with the permissions granted by the user. Developers that integrate with the Facebook Platform must adhere to terms that require them (among other things) to inform users of their privacy policy and to protect user information—by, for example, preventing the transfer of user information to third-party ad networks, data brokers, and the like. Although, as noted, applications that integrate with the Facebook Platform are designed and run by independent third-party developers, Facebook has devoted substantial resources to providing these developers tools that enable them to build safe and secure experiences. As just one example, last year Facebook adopted a new industry standard authentication tool called OAuth 2.0 that makes it easier for third-party developers to integrate with the Facebook Platform in a way that protects user information.

The potential security issue identified by Symantec involved the use of an older authentication API that pre-dates OAuth 2.0. Unlike OAuth 2.0, the older API required developers to take an extra step to ensure that information that a user’s browser passed to the application could not, in turn, be passed to third parties that provide content or other services on the application’s landing page. This requirement, which was not technically complex, was outlined in Facebook’s developer documentation, and the overwhelming majority of developers took this step and were thus unaffected by the issue Symantec identified. Some developers, however, did not take this step. As a result, some applications that had integrated with the Facebook Platform were inadvertently permitting users’ browsers to transmit access tokens to third parties. As noted above in footnote 1, an access token is a lengthy string of characters that enables the application to obtain from Facebook the information the user has explicitly authorized the application to obtain, and that permits the application to take other actions permitted by the user. The vast majority of access tokens (more than 90%) expire within two hours of their issuance. Some access tokens, however, provide applications offline access—meaning the user has given the application permission to access information or take other actions even when the user is not currently using Facebook (as for example, when an application enables the user to feed activity on the application back onto his Facebook profile page). Such offline access tokens do not expire after two hours. A third party in possession of such offline access tokens could, in theory, have used the access token, for example, to obtain access to the user information that the user had authorized the application to obtain.

As noted at the outset, and as Symantec itself has emphasized, the issue identified by Symantec was a theoretical one. Even today, after an extensive investigation, we are aware of no instance in which a third-party used an access token obtained through this mechanism in order to access a user’s account. Indeed, third-party ad networks that serve ads on applications that integrate

with the Facebook Platform—which the Symantec report identified as a possible source of misuse of access tokens—are bound by our terms not to obtain or use Facebook user information and have certified that they do not have such information.³ That said, as in all cases in which we learn of a potential security vulnerability—either through our own efforts or through the efforts of security researchers or others—we took aggressive action as soon as we learned of the issue. Symantec contacted us by email on April 13, 2011. Within two days we had taken steps to prevent any affected applications from continuing to expose access tokens to third parties through the process identified by Symantec. We also undertook a more expansive investigation of our platform to determine whether the issue identified by Symantec could affect any other developers, including developers of third-party websites that use the Facebook Platform to provide their users a more social, personalized experience. Through this investigation, we identified certain additional developers that may have been inadvertently allowing access tokens to be exposed to third parties, and we made clear that they needed to take steps to prevent such exposure immediately or be blocked from integrating with the Facebook Platform. We also accelerated the migration of developers to the OAuth 2.0 authentication API, which, as noted, addresses the issue Symantec raised and, more generally, makes it easier for developers to build secure applications and websites.⁴ Finally, we invalidated all offline access tokens that could have been exposed to third parties through the vulnerability identified by Symantec, thus preventing any third party that may have received such tokens in the past from using them to access user information.

We are confident that these steps addressed the vulnerability identified by Symantec. With this background in mind, I will now turn to your specific questions.

- 1. According to the *Wall Street Journal* article cited above, Facebook first learned of the leakage of the personal data of its users the second week of April 2011. Is that accurate? If yes, what steps did Facebook take to fix this problem? Did Facebook employ an outside firm in its effort to stop leakage? If not, why not?**

As described above, Symantec first contacted Facebook on April 13, 2011. By April 15, we had prevented any affected applications from exposing access tokens to third parties. Shortly thereafter, Facebook took the additional steps described above to prevent the vulnerability identified by Symantec from resulting in unauthorized access to user information, and we are unaware of any instance in which any user information was obtained by an unauthorized third party.

Facebook's investigation and resolution of this issue was handled jointly by members of our Security, Site Integrity, Engineering, and Platform and Developer Relations teams. These teams include security experts, engineers, analysts and other professionals who quickly assessed the problem and developed and implemented a solution. We did not employ an outside firm to assist in our investigation because we did not believe that one would result in a better or more expedient solution to the issue. As a general matter, we believe that our internal experts, who work with our

³ <https://developers.facebook.com/adproviders/>; https://developers.facebook.com/ad_provider_terms/.

⁴ <https://developers.facebook.com/blog/post/497>.

products and our code day in and day out, are in the best position to use the technological tools we have available to conduct an investigation and to find and implement the most appropriate fix. In this case, it would have taken longer to teach an outside firm how to use our systems than to perform the investigation and address the issue internally right away.

- 2. The article above states that “hundreds of thousands of applications may have inadvertently leaked millions of access tokens to third parties.” Is this consistent with Facebook’s understanding of the extent of the data leakage? If not, why not, and what is Facebook estimate of the magnitude of the data leakage?**

As discussed above, we are unaware of any instance in which the issue Symantec identified resulted in unauthorized access to user information by any third party, so to characterize this as a “data leakage” is, in our view, incorrect. Symantec likewise has observed that “to [Symantec’s] knowledge, no Facebook users were impacted by this issue.” And the steps described above ensure that any access tokens that were exposed to third parties are now nothing more than a meaningless series of characters with no intrinsic meaning or utility.

- 3. A Facebook spokesperson is quoted in the report as stating that Facebook’s thorough investigation of this matter had turned up “no evidence of this issue resulting in a user’s private information being shared with unauthorized third parties.” How was this investigation conducted? Was it conducted exclusively by Facebook? Was Facebook’s determination validated by a third party? If yes, which one(s)? Please explain.**

As mentioned above, a cross-functional internal team immediately collaborated to confirm the existence of the issue Symantec brought to our attention, to investigate the scope of the issue, and to develop and implement a solution: we immediately began investigating whether there was any evidence of misuse of access tokens or unauthorized access of user data associated with applications using the legacy API; we pulled information from our log files to determine which applications were potentially allowing access tokens to be exposed and how many access tokens associated with users were potentially affected; we conducted an initial manual audit of the top 50 applications, which have a combined total of more than 500 million users (not all of which were affected by this issue, since the bulk of the top 50 applications took the required steps to prevent the vulnerability and since most users do not grant applications offline access tokens); and our User Operations team reviewed user reports of applications to identify any reports that might suggest that third parties were using offline access tokens to obtain unauthorized access to user information or to take actions the user had authorized the application to take (such as posting to the user’s wall). Through all of these methods of investigation, we found no evidence of unauthorized access to user information. And, as noted, Symantec has stated that, to its knowledge, no users were affected by this issue.

- 4. In a company blog, Symantec researcher Nishant Doshi wrote that “[T]he repercussions of this access token leakage are seen far and wide... We fear a lot of these tokens might still be available in log files of third-party servers or still being actively used by advertisers.” What is Facebook doing to inform users of this**

problem? Has Facebook informed users that they can change their Facebook passwords to invalidate leaked access tokens, as recommended by Symantec? If not, why not?

Again, we have found no evidence that access tokens have been used to obtain unauthorized access to user information, and we have ensured that the vulnerability at issue will not result in any such access. At the same time, we agree that user education—about the importance of strong passwords, for example, and the importance of understanding the policies of the applications users choose to use—is critical. We recently launched a campaign on Facebook to educate people about how to make smart decisions about applications. This campaign includes pointing users to new materials on our Security Page⁵ and our Family Safety Center⁶ and reminding them to take care to understand the privacy policies and practices of the applications they choose to use.

5. According to the *Wall Street Journal* article, this data leakage persisted “for years.” Is this accurate? If not, what is Facebook’s estimate of the duration of this problem?

For the reasons discussed above, we do not agree with the characterization of this issue as involving “data leakage.” It is likely, however, that some applications that had not taken the steps necessary to prevent users’ browsers from exposing access tokens to third parties were in operation for more than the last year. At the same time, it is important to stress that most applications had taken the appropriate steps, that in any case the vast majority of access tokens expire shortly after their issuance, that in all events Facebook has taken steps to prevent this security vulnerability from leading to actual unauthorized access to user information, and that there is no evidence of any such unauthorized access resulting from this issue.

6. Is this data access for third parties a violation of Facebook’s privacy policy? In Facebook’s October 29, 2010 response to our October 18, 2010 correspondence, Facebook indicated that Facebook had “[I]dentified fewer than a dozen developers that were intentionally sharing User IDs (UID) with a data broker, in violation of our terms.” Did any of these developers have access to Facebook users’ information as part of the data leakage that is the subject of today’s *Wall Street Journal* article? If yes, which ones?

Facebook’s developer terms prohibit developers from enabling unauthorized third-party access to user information. Developers that failed to take the steps necessary to prevent exposure of access tokens to third parties were therefore in violation of our terms. Likewise, although we are not aware of any third party that used access tokens exposed in this manner to obtain unauthorized access to user information, if any ad network had done so, it would have been in violation of the ad network terms referenced above (as well as the certification ad networks have provided that they do not have and will not obtain Facebook user information).

⁵ <https://www.facebook.com/security>.

⁶ <https://www.facebook.com/safety>.

It should be stressed that in every case of which we are aware, applications' exposure of access tokens to third parties in the manner highlighted by Symantec was inadvertent. As the question notes, last fall we identified a very different matter: we learned that fewer than a dozen applications were intentionally passing the user IDs of Facebook users to a data broker. Facebook disabled the offending applications and required the developers of those applications to undergo an audit prior to launching applications in the future. Since then, a few of the developers have launched applications, and those applications obtain and use user information to the extent users have authorized them to do so.

- 7. In Facebook's response to our October 18th correspondence, Facebook indicated that the company "[E]mploys a dedicated Platform Operations team and a suite of sophisticated tools to detect and prevent third party applications from violating Facebook policies." Is the problem described in today's Wall Street Journal within the scope of responsibility of this team? If not, which Facebook team is responsible? Was the suite of tools described in Facebook's October 29th response to our correspondence applied to this matter? If not, why not?**

The Platform Operations team, along with User Operations, Site Integrity, and Security, are responsible for keeping our platform safe and secure and investigating any violations of our policies that they discover or that are brought to their attention. We are also grateful for the efforts of Symantec and other security researchers, who work very hard to identify and bring to our attention any vulnerabilities that may exist so that, as in this case, we can address them before they are exploited by bad actors in the ecosystem. Had Symantec not identified the issue, had we not identified it through our own ongoing security review of the Facebook Platform, and had a third-party exploited the vulnerability to obtain unauthorized access to user information, it is likely that such access would have triggered the tools I described in my prior correspondence (such as the platform enforcement tool, which monitors a range of application activity and flags anomalous behavior). In other words, the fact that our monitoring tools and systems were not triggered is further evidence that the vulnerability identified by Symantec was not exploited prior to our resolution of the issue.

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

Sincerely,



Marne Levine
Vice President, Global Public Policy