facebook

October 29, 2010

The Honorable Edward J. Markey
U.S. House of Representatives
Co-Chairman
Bi-Partisan Privacy Caucus
2125 Rayburn House Office Building
Washington, DC 20515-6115

The Honorable Joe Barton
U.S. House of Representatives
Ranking Member
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: Your Letter of October 18, 2010

Dear Chairman Markey and Chairman Barton,

I write to respond to your letter regarding the October 18, 2010, *Wall Street Journal* article involving the presence of Facebook user IDs ("UIDs") in the referrer URL of applications provided by third parties on the Facebook Platform. In this letter we first provide important information that adds context to the issue discussed in the *Wall Street Journal* article. We then respond to each of the 18 questions posed in your letter.

First, as a threshold matter, and notwithstanding the title of the *Wall Street Journal*'s article, the sharing of UIDs by Facebook with third-party applications does not involve the sharing of any private user data and is in no sense a privacy "breach." On the contrary, the sharing of UIDs is critical to people's ability to use third-party applications on the Facebook Platform. The Facebook Platform is designed to enable third-party developers to create innovative, social experiences for people. As a result, a thriving ecosystem of thousands of companies delivering value to tens of millions of people has developed.

When a Facebook user authorizes an application, he or she agrees to share certain information with the application – including his or her Facebook UID – so that the application can provide an innovative, social experience. As Facebook's privacy policy explains, "[w]hen you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, UIDs, connections, and any content shared using the Everyone privacy setting." Furthermore, as we discuss in more detail below, whenever a Facebook user authorizes an application, we remind

that person in real time what specific information the application will have access to, including the user's UID, and the user must specifically grant permission to the application to access the user's UID before using the application. Accordingly, any suggestion that the act of passing a UID to a third-party application is a "breach" of that user's privacy is false.

Second, the primary issue highlighted by the *Wall Street Journal* article – which is the inadvertent sharing of UIDs, not by Facebook itself, but rather by applications – is a by-product of how Internet browsers work. When a Facebook user visits an application that was created using a certain type of technology (known as an "i-frame"[1]), the URL embedded in the i-frame for that application includes, among other information, the user's UID, as described and disclosed above. If that application, in turn, relies on a third party to supply content or services for the application, it will instruct the user's browser to ask that third-party for the information it needs to operate. In making that request, the user's browser will often include the "referrer URL" – *i.e.*, the URL of the i-frame in which the application is running. Where that URL includes the UID, in turn, the party receiving that browser request may receive the UID as part of the string of information embedded in the URL. But that is not a Facebook-specific issue; on the contrary, it is simply because, in the course of its normal operation on the Internet, the browser includes the referrer URL in its request to the third party. Indeed, as many commenters observed in the wake of the article[2] – and as the *Wall Street Journal* emphasized in a subsequent article[3] – the issue is not Facebook-specific, but rather affects any number of sites and services that rely on third-parties to serve content or services. Nevertheless, we understand the reasons the inclusion of a UID in a referrer URL might make people who use Facebook uneasy, which is why we are in the process of making a technical change to address this issue, as described in more detail below.

Third, a Facebook UID at most enables access only to information that a user has already chosen to share and make publicly available. No information that a user has restricted using Facebook's privacy controls is available solely with a Facebook UID, including to applications or any third parties providing services or content to applications. Furthermore, Facebook employs technical measures to prevent third parties from using UIDs to obtain even the publicly available information of significant numbers of users.

---

[1] Most applications on Facebook Platform do not use i-frames and are thus not affected by the issue discussed in the *Wall Street Journal*'s article.

[2] *E.g.*, *Fear and Loathing at the Wall Street Journal,* http://techcrunch.com/2010/10/18/fear-and-loathing-at-the-wall-street-journal/; *Latest Facebook Privacy Scare Isn't So New*, http://voices.washingtonpost.com/fasterforward/2010/10/latest_facebook_privacy-news_s.html.

[3] *MySpace, Apps Leak User Data*, Wall St. J., Oct. 22, 2010 (in a follow-up article, explaining that "[t]he Journal's investigation demonstrates how *fundamental Web technologies* can jeopardize user privacy.") (emphasis added).

Fourth, we recognize and accept our leadership position and have already announced plans for a mechanism that will prevent UIDs from being transmitted to applications via URL, and which in turn will prevent the inadvertent passing of UIDs via referrer URLs. We are actively developing this mechanism and plan shortly to deploy it. But we are not stopping there. As noted, the passing of information via referrer URLs is an industry issue. We are working to launch an industry-wide initiative to equip browsers with privacy controls that would prevent such inadvertent passing of information. This is a complex technical question that calls for a technical answer – principally, we believe, one that should be provided by browser manufacturers. In the coming months, we expect to work with such manufacturers to enable users to control the passage of information via referrer URLs.

Fifth, although, as noted, a UID provides access only to information a user has chosen to share and make publicly available, and although we have seen no evidence to suggest that ad networks were or are using UIDs to obtain even this basic information, we see no reason for ad networks to store such UIDs. We therefore are mandating that all ad networks delete any Facebook UIDs they may have stored as a precondition to their continued ability to operate on Facebook Platform.

Finally, in the course of investigating the inadvertent sharing of UIDs highlighted by the *Wall Street Journal*, we identified a handful of applications that were intentionally sharing UIDs with a third-party data broker. This is a direct violation of our terms, and one we take very seriously. We have taken (i) enforcement action against the applications in question, and (ii) steps to ensure the deletion of the Facebook user data that was improperly transferred. The third-party data broker in question has also agreed not to operate on Facebook Platform in the future. These steps are explained in the attached blog post, which we released earlier today.

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

1. **How many users were impacted by the series of privacy breaches discovered by the Wall Street Journal?**

As the above explanation should make clear, the sharing of UIDs with applications is not a privacy breach, but rather is necessary to enable Facebook users to enjoy various third party applications. Further, Facebook explains to users – both in our privacy policy and at the time a user authorizes an application – that the application receives their UID, and users must specifically grant permission to applications to access their UID before using an application. Beyond that, where a user's browser passes a referrer URL that includes a UID to a third-party that provides content or services to an application, the UID does not enable that third party to obtain any information beyond that which the user has shared and made publicly available, and we have technical measures in place to prevent third parties from using UIDs to obtain the publicly available information of a significant number of users.

**2. What was the specific nature of the information transmitted from the third party application to other parties?**

The primary issue in question involves the transmission of a referrer URL of a third-party application from a user's browser to a third-party content or service provider for that application, with a user's UID embedded in the URL.

**3. When did Facebook become aware of this series of privacy breaches?**

The *Journal* contacted Facebook regarding its article prior to the release of the online version on October 17, 2010. We first learned that an application developer might be intentionally transferring UIDs to a data broker on October 14, 2010. Upon confirmation of that fact on October 15, we immediately suspended the operation of that developer's applications and initiated the investigation that resulted in the enforcement action noted at the outset and explained in the attached blog post.

**4. Did you notify your users of this series of breaches, including the specific nature of the information shared without their consent? If not, why not?**

We advise users – both in our Privacy Policy and in the disclosures we provide to users each and every time they authorize a new application – that applications they use will have access to their UID. We also advise users in our Privacy Policy to "review the policies of third party applications and websites to make sure you are comfortable with the ways in which they use information you share with them." Finally, we disclose to users that information that users share with "everyone" is available to everyone on the Internet. For example, in our Privacy Policy, we explain that information shared with "everyone" can "be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third party search engines, and be imported, exported, distributed, and redistributed by us and others without privacy limitations."

**5. What terms contained in your privacy policy were violated by this series of privacy breaches?**

As explained above, the disclosure of a user's UID to an application is essential to the operation of the Facebook Platform, and we specifically inform users – both in the Privacy Policy and elsewhere – that applications they authorize will receive their UIDs. There has therefore been no breach of our Privacy Policy. In the few instances where applications intentionally transferred UIDs to a third-party data broker, those applications violated section 9.2.6 of our Statement of Rights and Responsibilities ("SRR"), which prohibits applications from transferring user data to, *inter alia*, data brokers.

**6. How many third party applications were involved in this series of privacy breaches?**

For the reasons explained above, the sharing of UIDs with applications is disclosed both in our Privacy Policy and at the time a user authorizes an application; it is not a privacy breach. However, as noted above, in the course of our investigation, we identified fewer than a dozen developers that were intentionally sharing UIDs with a data broker, in violation of our terms. We have taken enforcement action against those developers, and we have taken steps to ensure that all Facebook user data passed to the data broker in question is deleted.

**7. What procedures do you have in place to detect and/or prevent third party applications that may breach the terms of Facebook's privacy policy?**

Facebook requires applications to have their *own* privacy policies, and, in section 4 of our Privacy Policy, we encourage users to review applications' privacy policies to make sure the users are comfortable with the ways in which the applications use information shared with them. We also require applications to link to their own privacy policy when they ask users to authorize the application, so that the user can review the application's privacy policy before deciding whether to authorize the application. We do not as a matter of course investigate applications' compliance with their own privacy policies, but we do require in our terms that applications adhere to their policies, and we take enforcement action where we learn of violations. In addition, and as detailed below, Facebook employs a dedicated Platform Operations team and a suite of sophisticated tools to detect and prevent third party applications from violating Facebook's policies.

**8. Have there been similar privacy breaches by third party applications in the past? If so, please describe the nature of those breaches. Please also describe any measures you may have put in place following the discovery of any such breaches to guard against future breaches and to better protect consumer privacy.**

The inadvertent passing of UIDs via the referrer URL of an i-frame application is not a breach of user privacy. Regarding the intentional transmission of UIDs to a data broker, this is the first instance in which we have learned of such activity, and, as noted, we have taken decisive enforcement action.

**9. What guidelines does Facebook have in place for third party applications to protect its users from advertent or inadvertent privacy breaches?**

Facebook's SRR and its Platform Policies establish policies to which applications must adhere in order to operate on the Facebook Platform. These policies are constructed around a set of basic principles that govern the Platform, among which is the requirement to "Be Trustworthy." Consistent with that principle, Facebook requires, among other things, that application developers request only data they need to operate their application; create (and

adhere to) a privacy policy that informs users how the application uses user data; honor user requests to delete information; and refrain from selling user data and from transferring user data to ad networks, data brokers, and other specified entities. The full text of Facebook's SRR is available at http://www.facebook.com/terms.php, and the Platform Policies are available at http://developers.facebook.com/policy/. In addition, both documents are included with this letter.

**10. Please identify the officials or offices within Facebook who are responsible for ensuring that third party applications satisfy Facebook's terms and conditions. What is Facebook's procedure for reviewing third party applications to ensure they satisfy Facebook's terms and conditions?**

Numerous organizations, involving potentially hundreds of people, participate in monitoring and enforcing compliance with Facebook's developer terms. Facebook's engineering team, for example, is responsible for building and maintaining the automated tools that ensure that applications are able to access only information that a user has authorized. Likewise, complaints relating to applications are handled through Facebook's dedicated Platform Operations team, which works with numerous organizations across the company – such as engineering, security, business development, public policy, and legal – as necessary depending on the issues in question. The Platform Operations team itself consists of 36 full-time employees, 23 of whom devote 100% of their time to monitoring and enforcing Facebook's policies with third-party applications. Since it was formed in 2007, this team has enforced Facebook's policies against hundreds of thousands of applications. Platform Operations employs a variety of steps and processes to monitor, test, or audit applications that are built on the Platform. Below we identify the general processes and tools utilized when performing these functions.

*Pre-Launch Documentation and Procedures*

Before a third-party developer creates and/or launches a Platform application, information about Platform and guidance is available on Facebook's developer web site, located at http://developers.facebook.com. The material on this site explains Facebook's policies, and instructs developers how to develop Facebook applications and access data in compliance with those policies.

In order to launch an application on Facebook, developers must first register as Facebook users, which requires affirmative acceptance of Facebook's SRR. The SRR requirements that apply specifically to developers are set out in Section 9 of the SRR and include the requirements described above (among others). As noted, developers must also adhere to the policies set out in the Facebook Platform Policies. Facebook also uses automated tools to prevent the creation of (and to auto-delete) fake accounts, which help to ensure accountability among application developers. In addition, Facebook uses automated tools to screen each application for improper

content and to detect (and block) any applications associated with an extensive blacklist of malicious URLs.

*Ongoing Review of Applications*

The Platform Operations team subjects hundreds of applications each month to a detailed review. The company focuses its systematic review of individual applications on those responsible for the majority of user experiences on Platform. Depending on operational constraints, certain applications may be reviewed as often as every four to six weeks.

When reviewing a specific application, Facebook relies on various tools described below, and in addition conducts a thorough review of the application's functionality and operation to assess compliance with Facebook's SRR and Platform Policies. This includes a thorough review of the application's operation and content.

*Investigations Based on Reports and Leads*

In addition to its systematic review of applications, Facebook relies on reports from users, complaints received via email, tips from Facebook employees, reports from other application developers, investigative leads uncovered by Facebook's security team, and other sources to identify potential areas of concern with specific applications. Facebook includes a "Report Application" link on the bottom of each application's page to make it easy for users or others to report concerns about a particular application. In addition, Facebook has created various automated tools that identify applications that are receiving a high volume of complaints.

Platform Operations reviews applications that are reported or otherwise brought to its attention through these means in the same manner described above, and as appropriate given the nature of the complaints or concerns relating to the applications.

*Monitoring and Enforcement Tools*

In addition to manual review of specific applications, Facebook uses a series of automated reporting and enforcement tools that allow it to quickly identify and respond to potential violations of its policies. Platform Operations reviews applications flagged by these tools and, if policy violations are discovered, documents those violations and escalates the issue for resolution.

**Monitoring Tools.** Facebook uses several automated tools to monitor a wide range of operational data and activity on Platform. Facebook personnel work in shifts to review the output from these tools and to investigate applications displaying abnormal or potentially abusive behaviors. Among other automated tools:

- Facebook monitors enforcement activity through a dashboard system, which provides a real-time view of identified issues, outstanding enforcement actions, and activity by applications under review.

- Facebook also employs a platform enforcement tool which aggregates and displays several metrics concerning the activities of applications on Platform, including how many users they have, how many data requests they are sending, whether the application is generating any complaints or spam reports, what types of data it is requesting of users, etc. This tool also displays this data in various statistical formats, which allows identification and assessment of outlying behaviors.

- Facebook uses a data access tool that tracks real-time data pulls and rates and provides historical and trend information, giving Facebook a view into applications' patterns of access to user data.

**Site Integrity Tools.** Facebook's Site Integrity group maintains an array of tools that monitor and protect Facebook.com generally against malicious conduct. For example, Site Integrity identifies IP addresses that are the source of malicious behavior and blocks all access to Facebook from those IP addresses. Site Integrity also protects users by monitoring, and in certain instances taking action against, new, fast-growing applications that match characteristics indicative of improper behavior. While these tools are not application specific, they assist in the protection of the Platform user experience.

*Escalation and Enforcement*

Facebook addresses policy violations through measures that take into account the nature of the violation, the application's history and usage, additional violations, and other factors. Facebook's approach to enforcement is intended to establish a consistent approach to applications that fail to comply with Facebook's policies. As a general matter, the initial response for minor policy violations is to inform the developer and set a deadline for the application to be brought into compliance. For more serious violations, repeated violations, or where the compliance deadline has not been met, Facebook typically will place the application under one or more moratoriums. For example, an application that exhibits a serious policy violation may receive a moratorium on its use of Facebook's communication channels – *i.e.*, the mechanisms that applications use to communicate with Facebook users. Because the use of communication channels is critical to the success of applications built on the Facebook Platform, the imposition of such moratoriums has a significant deterrent effect on policy violations. Applications that present the most serious issues are disabled entirely, as are applications that fail to establish compliance after notification and moratoriums. In a few cases, Facebook has banned developers from participating on Platform altogether. In addition, where appropriate, Facebook has taken legal action in response to Platform policy violations.

**11. Please provide copies of any agreements between Facebook and its third party application developers.**

We have attached to this letter a copy of our SRR and Platform Policies. We have also included a copy of our Privacy Policy. We have separate stand-alone agreements with certain individual developers, but with respect to the transfer and use of user data, the terms in those agreements generally mirror our standard terms.

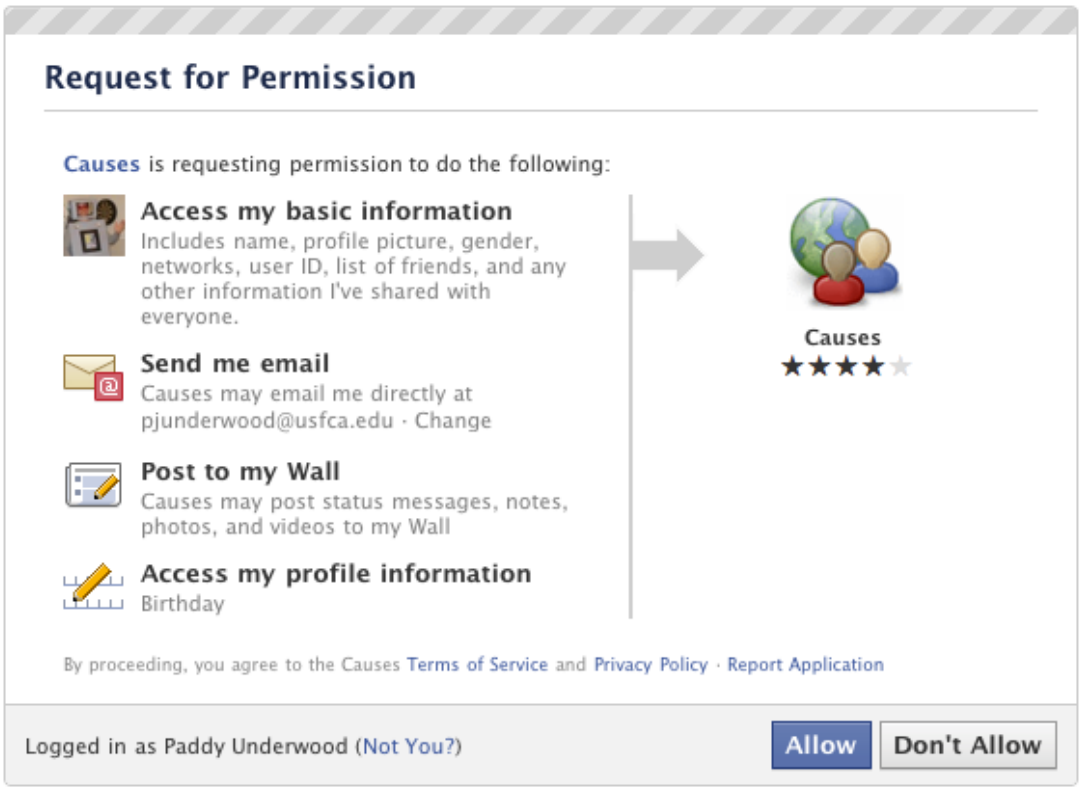
**12. Does Facebook receive any remuneration, financial or otherwise, as a result of the sharing of information between third party applications and internet tracking or advertising companies? If so, please disclose the nature and amount of the remuneration paid to Facebook.**

Facebook does not receive any remuneration, financial or otherwise, as a result of any sharing of information between third-party applications and Internet tracking or advertising companies. On the contrary, Facebook expressly prohibits application developers from selling user data and from transferring user data to such companies.

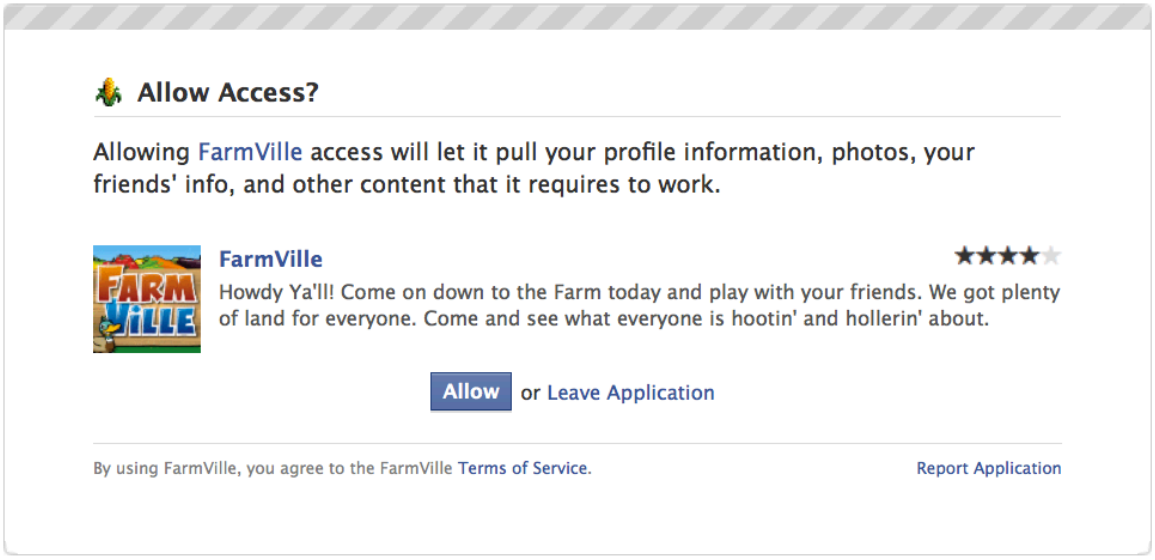
**13. For each application, please provide a copy of the terms and conditions or notice that was presented to the user before using the application. If multiple versions have been used, please provide all versions and note their dates of use. Please also identify any specific terms violated in this series of breaches.**

As noted above, Facebook's Privacy Policy informs users that, when they authorize an application, the application will have access to their UID (among other information). We have included a copy of our Privacy Policy with this letter.

In addition, as also noted above, at the time of application authorization, Facebook provides users a disclosure making clear that the application will obtain access to user information it needs to work, and requiring the user to grant permission for the application to access that information before the application may do so. This disclosure has changed over time. Currently, each application presents a dialogue box containing the categories or items of data the application is requesting access to, as well as a hyperlink to the application's privacy policy (and, in many cases, its terms of service). An example of this disclosure is set out below:




Prior to the development and deployment of the current permissions model shown above, applications provided a more general disclosure (though one that also made clear to users that the application, if authorized, would receive user information). An example of that disclosure is shown below:



**14. Will Facebook seek the deletion of its users' personal information from data bases of the internet or advertising companies who received it as a result of this series of privacy breaches? If yes, when? If not, why not?**

Yes, we are currently taking steps to ensure that all ad networks and data brokers that may have stored UIDs obtained from applications as a result of the issues discussed in this letter delete those UIDs. More generally, as part of our normal course of business, Facebook investigates allegations of third-party access to Facebook user information and takes aggressive action where it determines that third parties have obtained and are using Facebook user information in violation of Facebook's terms.

**15. To what extent has Facebook determined that data relating to minors 17 years of age and under were breached?**

We do not believe that data relating to any user, including minors, was breached via the passing of referrer URLs. Moreover, a UID cannot be used to obtain information about a user's age or birthday or other information that would identify the user as a minor.

Minors can and do use applications on Facebook, and, consistent with our Privacy Policy and other disclosures, their UIDs are shared with applications when they do. Facebook does, however, have in place certain measures that limit sharing of minors' information, even where that minor makes that information available to everyone. First, minors do not have a public search listing created for them that would enable their public profile information to be found on search engines. Second, content that minors share using the "everyone" setting is in fact shared with a more limited audience (friends, friends of friends, and verified networks) until the user turns 18. Accordingly, a UID would not enable access to such information until the user turns 18.

**16. To what extent has Facebook determined that personal financial or medical data were breached?**

No private information was shared through the issues discussed in this letter.

**17. Please describe any policy or procedure changes Facebook plans to adopt to ensure that users have better control over how their information is shared and with whom their information is shared when using third party applications.**

Facebook is always innovating to build tools that give users greater control over how their information is shared, including with third party applications. Earlier this year, we deployed an extended applications permissions model which gave users greater granularity in the approval process that is required before they can share their information with applications. Likewise, Facebook recently announced an audit feature that enables users to see which

applications they have previously approved to receive information about them, the specific types of information users have authorized Facebook to share with the application, and the most recent dates the application has requested this information. We also offer an immediate mechanism for users to remove the authorization if based on the audit trail they no longer wish to share information with the application. More recently, as discussed in the attached blog posts, we are developing a technical mechanism to prevent browsers from inadvertently passing UIDs to third-party content or service providers operating on Facebook Platform; we are launching an industry-wide effort to equip browsers with tools that will give users more control over what they share when they travel the Internet; we have reminded application developers of their obligation not to share Facebook user information in a way that is inconsistent with our terms or their own policies; and we have built a tool to help developers accomplish that goal while still delivering innovative and valuable social experiences for users.

**18. Please describe any changes Facebook plans to adopt in the terms and conditions or notices presented to users before using third party applications.**

Facebook currently informs users – both in our Privacy Policy and at the time of application authorization by a user – that using an application involves sharing certain information with the application, including the user's UID, and users must specifically grant permission to an application to access that information before using an application. We also encourage users to review application's privacy policies to ensure they are comfortable with how the application uses the user's information, and we monitor applications to ensure that they display clear and functioning links to their privacy policies to users. At the same time, we are communicating with our application developer community in order to make unmistakably clear that transferring any user information to data brokers of any kind is not allowed, and that the intentional sharing of UIDs is likewise impermissible. I have attached a blog post we released today that communicates these and other related points to our developers.

****

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

Sincerely,

/s/

Marne Levine
*Vice President, Global Public Policy*

Attachments:

FB DPP 10302010.pdf
Facebook Platform Policies (Updated – 10/20/2010)

FB-PP.pdf
Facebook Privacy Policy

FB-SRR.pdf
Facebook Statement of Rights and Responsibilities

FBdevblog-EncryptingUIDs 102110.pdf
Facebook Developer Blog Post, "Encrypting Facebook UIDs"

FBdevblog-UIDupdate 102910.pdf
Facebook Developer Blog Post, "An Update on Facebook UIDs"

TechCrunch-FearAndLoathing.pdf
TechCrunch, "Fear And Loathing At The Wall Street Journal"

WaPo-LatestFBPrivacy.pdf
The Washington Post, Faster Forward, "Latest Facebook privacy scare isn't so new"

WSJ-MySpaceAppsLeak.pdf
The Wall Street Journal, "MySpace, Apps Leak User Data"