FACEBOOK STATEMENT – RICHARD ALLAN – NOVEMBER 11, 2013

[I. INTRODUCTION]

My name is Richard Allan, and I am the Director of Public Policy for Facebook in Europe, the Middle East and Africa.

I have been with Facebook since 2009 working on a wide range of policy issues across the region.

I am grateful for the opportunity to be able to appear before the Committee on Civil Liberties, Justice and Home Affairs.

In my introductory remarks, I would like to cover 3 areas –

1) a brief description of Facebook as a service;

2) our policies and practices with respect to requests for data from government agencies; and

3) recent reports about government surveillance activities.

[II. BACKGROUND]

Facebook's mission is to help give people the power to share and to make the world more open and connected. Facebook recently reported that more than 1.2 billion people are using Facebook on a regular basis across the globe, including many people throughout Europe. Each month, Facebook enables every one of these users to

share information – photos, videos, status updates, and messages – with their friends and family. It is therefore vital that Facebook retain the trust of the people who use our service and maintain the security of their data.

Facebook's Statement of Rights and Responsibilities and Data Use Policy establish Facebook's relationship with the people who use our service. Facebook provides extensive assistance to promote understanding of these policies and ensure that people are able to make use of the available privacy controls to share information in accordance with their personal preferences. Facebook offers a comprehensive online Help Center and a large User Operations team (or customer support) that is available to people throughout the world. This team, many of whom are based in Dublin, ensures that we can protect the safety and privacy of people using our service in accordance with our policies. The User Operations team evaluates reports from people who use Facebook 24 hours a day and will take appropriate action against any abuse they find.

Facebook also has a strong security team headed up by our Chief Security Officer who ensure that we have the right technology, policies

and processes in place to keep our service and people who use it as secure as possible. Examples of technologies they have deployed include encrypting all user connections to Facebook by default and sophisticated systems to detect unauthorized access to a user account.

Facebook is a global company. People from over 100 countries regularly share and connect with our service. The Facebook service is provided to European users by Facebook Ireland, our international headquarters outside of the United States. Facebook Ireland is regulated under the terms of the existing 1995 European Data Protection Directive by the Office of the Data Protection Commissioner in Ireland.

We have around 500 staff in our Dublin office who cover a wide range of headquarters functions and support users and customers in multiple languages. We have established other smaller offices in a number of EU countries whose main function is to assist Facebook Ireland in promoting its advertising products to business customers.

[III. DATA REQUESTS: POLICIES AND PRACTICES]

Let me turn now to Facebook's policies and practices on data disclosure. Facebook has developed well-established processes for law

enforcement and governmental authorities around the world to submit data requests. These processes are described in guidelines that we have published publicly on our site. Law enforcement authorities in Europe and elsewhere around the world can submit requests for data in official investigations directly to Facebook through Facebook's Law Enforcement Online Request System at www.facebook.com/records, by fax or by post to Facebook Ireland. To ensure that these processes are well-understood, Facebook representatives have provided guidance and training for police officers in Europe, particularly those who focus on Internet and child safety.

Facebook has stringent processes in place to handle all government data requests. Facebook believes this process protects the data of the people who use Facebook, and requires all governments to meet a high legal bar. Facebook scrutinizes each request for legal sufficiency under its terms and the strict letter of the law, and requires a detailed description of the legal and factual bases for the request. Facebook pushes back when it finds legal deficiencies and fights many of these requests, and is often successful in narrowing the scope of overly broad or vague requests. In many cases, Facebook is required to

share only very limited data about an account, such as basic subscriber information.

Facebook is able to respond expeditiously to many European requests, including cases where there is an imminent risk of death or bodily harm. For instance, Facebook has worked with law enforcement authorities in child abduction cases to assist in locating the missing child.

The activities of Facebook Ireland's Law Enforcement Response Team have been examined by the Office of the Data Protection Commissioner during his audit of Facebook Ireland and his follow-up report of 21st September 2012.

During the September 2012 review, the Data Protection Commissioner found that all of the requests they examined met the conditions in the Irish Data Protection Acts. They also stated their view that "FB-I(reland) is appropriately assessing requests and either seeking additional information or justification where it has concerns or is refusing such requests".

[IV. REPORTS ABOUT GOVERNMENT SURVEILLANCE]

Over the past several months, there's been a great deal of media

coverage and interest in the nature and extent of government requests from online providers in national security investigations, and how companies like Facebook respond to these requests. Much of this coverage has been inaccurate or misleading. Facebook has therefore taken a number of concrete steps to address these concerns.

First, Mark Zuckerberg, founder and CEO of Facebook, has forcefully and repeatedly rejected false reports that Facebook had somehow allowed "direct" or unfettered access by any government to Facebook data. As he stated the day after these news reports first surfaced:

> "Facebook is not and has never been part of any program to give the US or any other government direct access to our servers. We have never received a blanket request or court order from any government agency asking for information or metadata in bulk. And if we did, we would fight it aggressively."

Second, Facebook has released the maximum amount of information allowed by law concerning the government data requests it has received. In June, about a week after these reports and after intense

negotiations with the U.S. government, Facebook released a U.S. government requests report that included all U.S. national security-related requests – which no company had been permitted to do before that time. These numbers showed the limited number of these data requests. For the 6 months ending December 31, 2012, the total number of user-data requests Facebook received from any and all government entities in the U.S. (including local, state, and federal, and including criminal and national security-related requests) – was between 9,000 and 10,000. These requests run the gamut of matters – from things like a local sheriff trying to find a missing child, to a police department investigating an assault, to a national security official investigating a terrorist threat. The total number of user accounts for which data was requested pursuant to the entirety of those 9-10,000 requests was between 18,000 and 19,000 accounts.

In August, we supplemented our disclosures of U.S. request data with a Global Government Requests Report that provided information on the total number of government requests for user data that Facebook had received from every country that submitted a data request for the first half of 2013. The report stated that the total number of US requests of all types was between 11-12,000, requesting information on 20-

21,000 accounts. Note that this US number includes any requests that have been made on behalf of third countries, including EU countries, through Mutual Legal Assistance Treaty arrangements. Through this MLAT process, a request is made to the US Department of Justice by the government of a country that is party to an MLAT arrangement and will be served on Facebook by a US court in a similar way to a domestic US request.

In addition, the report detailed the specific number of requests from each European country. The total number of requests that came directly from European Union countries for this period was 8,500. These requests targeted approximately 10,000 accounts.

With more than 1.2 billion monthly active users worldwide, these reports demonstrate that a tiny fraction of one percent of Facebook user accounts were the subject of any kind of government request in the past year. This helps put in perspective the numbers involved, and lays to rest some of the hyperbolic and misleading assertions we have seen about the frequency and scope of the data requests that Facebook receives.

Third, Facebook, along with others in industry, has been pushing the United States government for the ability to be even more

transparent about the government requests. In September, Facebook filed a legal action with the Foreign Intelligence Surveillance Court in Washington, D.C. seeking authority to disclose, at regular reporting intervals, the total number of national security orders it has received, if any; the total number of user accounts specified in such orders; and the number of requests seeking the content of communications versus those seeking transaction or subscriber information.

While transparency is a critical first step to an informed public debate, we believe that more needs to be done. In late October, Facebook joined several other providers in publicly calling for government surveillance practices to be reformed to include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for those programs. Together with a number of other companies, we sent a letter that applauded Rep. Sensebrenner, who I understand you have heard from today, and his colleagues for the important contribution to the debate that their legislative proposal represents.

[V. CONCLUSIDING REMARKS]

Facebook will continue to be vigilant in protecting our users' data

from unwarranted government requests, and will continue to ask all governments to be as transparent as possible.

We are very interested in the work of elected representatives around the world as they develop policy and legislation on access to Internet data. We believe that we have a common goal in wanting there to be widespread public trust in the way in which governments create and use their powers in this sensitive area.

In that spirit, we are happy to do what we can to help the European Parliament bring its expertise to bear on these complex questions. And I hope that this statement and my responses to any questions you have will help in that process.