Exhibit EE

June 16, 2010

An Open Letter to Facebook CEO Mark Zuckerberg

Dear Mark,

We are glad to see that Facebook has taken steps in the past weeks to address some of its outstanding privacy problems. However, we are writing to urge you to continue to demonstrate your commitment to the principle of giving users control over how and with whom they share by taking these additional steps:

1) Fix the "app gap" by empowering users to decide exactly which applications can access their personal information.

2) Make "instant personalization" opt-in by default.

3) Do not retain data about specific visitors to third party sites that incorporate "social plugins" or the "like" button unless the site visitor chooses to interact with those tools.

4) Provide users with control over every piece of information they can share via Facebook, including their name, gender, profile picture, and networks.

5) Protect Facebook users from other threats by using an HTTPS connection for all interactions by default.

6) Provide users with simple tools for exporting their uploaded content and the details of their social network so that users who are no longer comfortable with Facebook's policies and want to leave for another social network service do not have to choose between safeguarding their privacy and staying connected to their friends.

By addressing these outstanding issues, Facebook can continue to demonstrate its commitment to user privacy. We look forward to working with you in doing so.

The "App Gap"

One issue that must be resolved is the "app gap": the fact that applications and web sites that use the Facebook Platform can access a user's information if that user's friend—and not the user herself—runs the app or connects with the site.

Facebook's latest changes allow users a "nuclear option" to opt out of applications entirely. While this is an important setting, it is not adequate for meaningful control. Facebook users should also have the option to choose to share information only with specific applications.

"Instant Personalization"

Facebook recently announced "instant personalization," which allows specific partner web sites to access Facebook information as soon as a logged-in Facebook user visits that site—and *before* that user ever consents to having information disclosed to the site. To remedy this situation, "instant personalization" should be turned off by default, and users who want this feature should affirmatively consent. Similar to apps, users should also have the option to selectively choose Instant Personalization for particular web sites.

"Social Plugins"

Facebook has recently released a series of "social plugins," including a "like" button, that allow visitors to an external site to see how other Facebook users have interacted with that site. What has gone largely unannounced is that these plugins provide Facebook with information about every visit to the site by anyone who is logged in to Facebook, whether or not the visitor ever interacts with the plugins or clicks on the "like" button at all.

While we understand that Facebook is anonymizing this data after 90 days, Facebook should not retain any identifiable information for any period of time unless the site visitor actually interacts with Facebook's plugins or buttons. If Facebook wishes to retain aggregate or anonymized information for other purposes, as it states, it needs to make its anonymization procedure public so that its effectiveness can be evaluated. Facebook should also restore the button for logging out of Facebook to a prominent position in the main navigation bar, rather than placing it in a drop-down menu.

Full Control

According to one of Facebook's earliest privacy policies, none of your personal information was available to anyone who did not belong to at least one of the groups specified by you in your privacy settings. In past months, however, the idea of full control has eroded and been replaced with the concept of "publicly available information." Facebook has recently removed friend lists and connections from this category by restoring privacy controls for these fields—but other fields remain outside of the users control.

We urge Facebook to give users full control over who (or what) can see every piece of their information, including the fields that remain "publicly available," in keeping with its principle that "People should have the freedom to decide with whom they will share their information, and to set privacy controls to protect those choices." We also encourage Facebook to continue to streamline its privacy settings so that users can easily configure the settings for their personal information.

HTTPS

Facebook users communicate a wealth of private information—from personal messages and photos to the content they share with just a few friends—on the service. However, by default, this information is sent over the Internet in unencrypted fashion, potentially allowing it to be intercepted by other parties.

Facebook should protect this information from outside snooping by providing users with an easy HTTPS option and by turning that setting on by default. Doing so would further its commitment to user privacy.

Data Portability

Users should have control over the details of their social network and the content that they have uploaded to Facebook, and should be able to export and move that data to another service if they decide they are uncomfortable with Facebook's privacy policies. Facebook should demonstrate its commitment to user control by giving users easy tools for directly downloading their content and information about their social network, as other companies in the social networking space have already done.

"Privacy" and "social" go hand in hand: Users are much more social with people they know and choose, and much less social when their actions and beliefs and connections are disclosed without their control or consent.

We are committed to continuing this dialogue with you and ensuring that users can continue to be both social and private on Facebook. We hope you continue to engage with us and your users to make Facebook a trusted place for both public *and* private sharing. Please make the default "social—and private."

Sincerely,

ACLU of Northern California

Center for Democracy and Technology

Center for Digital Democracy

Consumer Action

Consumer Watchdog

Electronic Frontier Foundation

Electronic Privacy Information Center

PrivacyActivism

Privacy Lives

Privacy Rights Clearinghouse