



December 5, 2011

Honorable Joe Barton
United States House of Representatives
2109 Rayburn House Office Building
Washington, D.C. 20515

Honorable Edward Markey
United States House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515

Honorable Marsha Blackburn
United States House of Representatives
217 Cannon House Office Building
Washington, D.C. 20515

Honorable Carolyn B. Maloney
United States House of Representatives
2332 Rayburn House Office Building
Washington, D.C. 20515

Dear Representatives Barton, Markey, Blackburn, and Maloney:

I write in response to your October 28, 2011 letter inquiring about Facebook's data storage and deletion policies. Thank you for the opportunity to describe our practices.

At Facebook, we have built a global communications platform embraced by hundreds of millions of people because we give them the power to share and connect in the ways that they want with the audiences that they want. As we reiterated in our agreement last week with the Federal Trade Commission, we are dedicated to ensuring that the data consumers entrust to us is secure and that they can control its use and visibility. Our approach to data protection starts with our commitment in our Statement of Rights and Responsibilities: "You own all of the content and information you post on Facebook."

That pledge is reflected in the controls we build into Facebook that enable you to define the visibility of content on a per object basis and to later change your mind and alter the privacy setting of something you have previously posted. Facebook was founded on the idea of giving you control over who you share information with and making sure only those people you intend can see it, and we have adopted policies and procedures that reflect this commitment.

As our CEO Mark Zuckerberg explained in his blog post last week, our agreement with the FTC reflects a firm commitment to formalize and enhance our privacy and data security practices. We have always taken privacy and security seriously at Facebook, and we have worked hard to build people's trust. But we also recognize that we have made mistakes, and that it is important to learn from them. Under the framework we agreed to with the FTC, we will implement a privacy program that will formalize and enhance our internal processes to identify and address privacy and security risks on Facebook. This privacy program will be developed and administered by two highly qualified privacy experts — our Chief Privacy Officer, Policy, Erin

Egan, and our Chief Privacy Officer, Products, Michael Richter — who will ensure that our strong privacy commitments are reflected in how we develop and operate our products and how we interact with regulators, privacy advocates, and other stakeholders. They also will provide information about our privacy efforts to the FTC and to an independent outside auditor, who will be tasked with assessing whether we are meeting our obligations on a regular basis over the next twenty years. As both Mark and the FTC emphasized last week, our agreement with the FTC reflects emerging industry standards and, in that sense, helps to establish rules that all Internet-based companies can and should live by.

The protections, policies and procedures we follow and will implement moving forward all center on the core principle that Facebook should at all times reflect and embrace social norms about authenticity, friendship, trust, and sharing. We require, for example, that you use your real name on Facebook so that these social norms, which exist throughout our society, can play the same role online. This, in turn, helps ensure that the privacy settings and controls that we offer are meaningful and effective. Indeed, unlike with other parts of the Internet, where anonymity can engender callous conduct and where your reputation, information, and the content you share with others enjoy little protection, Facebook is designed around the concept of a community, where trust and accountability exist because your postings and interactions always are attributable. Of course, social norms can be broken when trust between individuals is misplaced, and no technology can protect against misplaced trust in a friend.

Promoting user control has always been a top priority at Facebook, and it is even more so today. Our agreement with the FTC sends the message that we are serious about continuing to build privacy into Facebook and that we are a leader when it comes to defining and embracing the standards that should define our industry, and it ensures that we will be held accountable if we do not live up to what we promise.

It is in this spirit that we provide more information below about our approach to storing and deleting data on Facebook in response to your specific questions.

1. Please describe all personally identifiable information that Facebook collects from its consumers.

When people use Facebook, they do so for the specific purpose of sharing with others. In order to use Facebook you need only provide us with your name, date of birth, email address and gender. Of course, we also act as the custodian of the information you share with others through the service. For example, when you add information to your profile page, such as your personal, educational and professional affiliations, we store that information so that we can display it when others to whom you have given permission look at the profile. Similarly, when you send a message to a friend, we store that message so that we can display it to that friend. Likewise, when people choose to become “friends” on Facebook (or to discontinue a friend relationship), we store that information so that we know how to manage the visibility of data between those people.

Disclosures about these and all of our other data collection practices are provided in our comprehensive Data Use Policy. The policy, available from almost every page on our site,

describes in plain English our data use practices and includes a comprehensive, easy-to-understand guide to privacy on Facebook. In it, we use a layered approach, summarizing our practices on the front page and then allowing you to click through the Policy for more details. From the same page, we offer interactive privacy tools that, for example, enable you to preview how your profile looks to any other specific person, see what permissions you've granted to the Facebook applications you use, and download the information you have submitted to Facebook all at once. Of course, if you want to read the entire Data Use Policy on one page, you can do that as well. And to ensure that we don't make changes to our terms that will catch people off guard, we engage in a notice and comment process to announce proposed changes and even will put changes to a vote if enough people comment adversely.

Part of our Data Use Policy contains a section called "Information we receive about you." That section provides details on the specific kinds of information that we receive from consumers, which includes:

- Registration information. When you sign up for Facebook, you are required to provide your name, email address, birthday, and gender.
- Information you choose to share. Your information includes the information you choose to share on Facebook, such as when you post a status update, upload a photo, or comment on a friend's post. It also includes the information you choose to share when you take an action, such as when you add a friend, like a Page or a website, tag a place in your post, find friends using our contact importers, or indicate that you are in a relationship.
- Information others share about you. We receive information about you from your friends, such as when they tag you in a photo, add a location to a post, or add you to a group. We also may receive information about you from the games, applications, and websites you use, but only when you have given them permission to share that information with us.
- Other information we receive about you. We receive other types of information about you, including data whenever you interact with Facebook (such as search for a friend or a Page) and data from the computer, mobile phone or other device you use to access Facebook (such as your IP address, location, the type of browser you use, or the pages you visit). We also receive data whenever you visit a game, application, or website that uses our service or visit a site with a Facebook feature. This data we receive in these instances may include the date and time you visit the site; the web address, or URL, you visited; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your Facebook User ID.

2. How is user information collected (i.e., initial sign-up process, usage of mobile phone application, etc.)?

We receive information when people interact with Facebook or one of our features, whether they do so using our website, using a Facebook mobile application, or using another method of communication like email or text messaging. Some examples of the ways in which we receive

information include when people sign up for Facebook; when they share information on Facebook (such as posting a status update); when they take an action on Facebook (such as adding a friend); and when they view Facebook web pages. We also make Facebook features available in other companies' products, such as in applications that they develop for Facebook or when they integrate Facebook features into their own websites, and we receive information when people interact with Facebook in those ways as well. As we describe above and in our Data Use Policy, the information that we receive includes the substance of Facebook posts themselves and some technical information about devices that people use to access Facebook, such as their Internet Protocol addresses, operating systems, and web browsers.

3. Please explain how Facebook stores this information (i.e., in a form that is encrypted or otherwise indecipherable to unauthorized persons)? How long is it stored? How does your company dispose of the information if at all?

Because securing information against unauthorized access is critical to Facebook, we invest heavily in technology, people and processes as part of our commitment to keeping data safe and secure. Facebook employs a full-time security team to develop, document, and implement security policies, and then monitor ongoing compliance with policies and respond to security incidents.

Facebook has a large network of geographically distributed single-tenant datacenters and goes to great lengths to protect the data in these centers. The geographic locations of the datacenters were chosen to give protection against catastrophic events. Only select Facebook personnel have access to the datacenter facilities, and this access is tightly controlled, audited and monitored.

On the information security side, we use a variety of techniques, including encryption, to protect various kinds of data that we store, and we rely on multiple layers of network segregation using firewalls to protect against attacks or unauthorized access. We customize our systems and servers to reduce the risk of unauthorized access and improve system performance. Applications are built using secure development practices that are designed to protect against hacking attempts from outside Facebook. Likewise, we have implemented procedures governing employee access to data, which include requiring special authorization based on job function before employees can access data and, once authorized, obligating employees to satisfy additional authentication requirements. We also closely monitor employee access to data to identify unusual behavior and prevent unauthorized activity.

Facebook also employs a full-time group within the security team that is dedicated to helping ensure security vulnerabilities are detected and addressed in a timely manner. The team actively scans for security vulnerabilities using commercial tools, intensive automated and manual penetration tests, code security reviews, and third-party internal and external audits. We also have adopted a "bug bounty" program that recognizes and rewards external security researchers that discover bugs and responsibly share them with us. Our program has received considerable recognition as an effective way to engage the broader security research community to promote a uniquely robust environment. And, if a vulnerability is identified, our security team is responsible for tracking the issue through remediation and validating the effectiveness of the fix.

We also bring a thoughtful approach to our data retention policies. Our policy is to make data retention decisions based on our understanding of the expectations of the people who use Facebook as well as the length of the time that we need the data to provide a quality experience on Facebook and to understand and improve the service we offer. As a result, our retention policies differ depending on the type of data and the intent of the people who use our service.

We already have a comprehensive process for responding to requests that we remove individual pieces of data, and we also will follow the obligations regarding this issue that are included in our agreement with the FTC, which are described in response to question 4. In addition, we use a standard procedure to dispose of deleted data on physical hardware. If we retain the physical hardware in which previously deleted data was stored, we re-use the hardware to overwrite the deleted material with fresh data. If we dispose of the physical hardware, we employ a data-destruction and verification procedure to help ensure the information is removed. This procedure consists of a single-pass overwrite, followed by a verification step. Once the drive has been verified, it is sent to our data destruction provider, which performs another single-pass overwrite and verification, then the vendor issues a Certificate of Data Destruction that identifies the serial number of the physical hardware from which the data was removed. If a drive fails the verification step at any point, it is crushed and then shredded in a further effort to prevent recovery of any data from the drive.

4. According to the article, it appears that Facebook does not delete information about a consumer when requested. What is Facebook’s policy for deleting information after the request of a consumer? Does Facebook delete any information upon request? If so, what information? If not, why not?

We respect people’s ability to request removal of information they have posted on Facebook and to request removal of their account in its entirety. This is reflected in the obligation that we undertook in our FTC agreement to

“implement procedures reasonably designed to ensure that [this] information cannot be accessed by any third party from servers under [our] control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity.”

In agreeing to this obligation, the FTC and we focused on our commitment that, when you ask us to remove information that you’ve posted, we act quickly to make that information inaccessible on Facebook. This commitment reflects the recognition that the fundamental goal of a removal request is to prevent further distribution of that information. The FTC recognized that the essential commitment to promptly make removed information inaccessible creates real value for consumers by giving them control over its further distribution.

Although the FTC requires that we make information you post on Facebook unavailable to third parties within thirty days after you request that we do so, we already use a process to prevent

information that you have posted from being accessible on Facebook almost immediately after we receive your request. We also go beyond our commitment to the FTC by not only making removed information inaccessible on our servers, but also taking steps to delete the information from all of our systems. Under this process, if you remove from your profile a piece of information such as a status update, photo or video that you have previously posted, we immediately remove the item from visibility on Facebook across all of the web servers we operate. At the same time, we also initiate a process designed to remove that information from other places where it may be stored in our systems, and we ask third party content delivery networks that may cache the information for your convenience to purge the data from their own servers.

As our agreement with the FTC reflects, there are some limited circumstances involving legal requirements or similar issues in which we are compelled to retain information. In these instances, we generally will remove the information from availability on the Facebook service but may retain it for a limited period of time in our records. We describe these circumstances in more detail in our response to question 6, below.

5. Please describe the technical challenges you face in responding to users' requests to remove data from the site.

Because we recognize that your ultimate goal when you request that we remove information you've posted from our site is to prevent others from seeing it, our first priority when we receive a removal request is to make the information inaccessible on our servers. As discussed above, this approach is reflected in our agreement with the FTC, which requires us to implement safeguards reasonably designed to ensure that we promptly render information that users have deleted from Facebook inaccessible to third parties.

But, as described above, we go beyond our FTC commitment to make information inaccessible by next taking steps to delete the information from our systems. This process can be challenging for companies like Facebook that operate large, distributed computing systems because information necessarily is stored in many places at once. For example, Facebook operates multiple data centers in different geographic areas, each of which stores copies of the information in Facebook's databases. Having data centers located near the people who use Facebook helps us provide access to Facebook without long delays. Using multiple data centers also provides redundancy, ensuring that Facebook will continue to function even if a single data center is receiving an unusually high amount of traffic, experiences a network problem, or becomes unavailable for another reason. We also store emergency backups of Facebook data in multiple locations to protect against data loss.

The consequence of this distributed architecture is that information you post on Facebook may be stored in multiple physical locations at once. This creates a significant engineering challenge for us because, if you ask us to delete your information, we have to do this not just in one place but also in multiple locations, which we may not be able to access instantaneously. We describe this process in our online Statement of Rights and Responsibilities, which says, "When you delete [content you post on Facebook], it is deleted in a manner similar to emptying the recycle

bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).”

Given the complexity of building deletion mechanisms that will work across our complex technical environment in a manner consistent with our policies and commitments, we have a multidisciplinary group of experts within Facebook that meets on a bi-weekly basis and works to address these technical challenges. We believe we have developed an industry leading process, but we continually work to identify changes in our procedures to maintain and increase their effectiveness, even as our service evolves over time.

6. Under what circumstances do you retain data after users request its deletion? How might consumers benefit from such retention?

As our agreement with the FTC reflects, in some limited circumstances we may retain information that people have posted to Facebook even if they request that we delete it. In some cases, we must meet legal obligations to preserve records for a period of time due to a litigation hold or regulatory requirement. For example, we take seriously our obligation to report suspected child exploitation to the National Center for Missing and Exploited Children and automatically preserve associated account records while an investigation by the appropriate authorities is ongoing. Likewise, if we receive a subpoena or other legal process or receive notification that certain account-related data relates to ongoing litigation, we may be under a legal obligation to preserve that information. As another example, we may delay deletion during our own investigations relating to safety and security threats to our users. If we receive a request to delete information but are not able to immediately implement the deletion process for one of these reasons or for some other technical reason, it is our policy to render that information inaccessible to third parties on the Facebook service and implement the full deletion process once we are able.

Like the categories of information that we maintain so that our security features work as designed, we also cannot delete certain information while your account is active to ensure our site features work correctly. For instance, we retain your history of actions around accepting and rejecting friend requests or removing someone from being a friend so we can make better decisions about whom to suggest to you as a friend. Likewise, if you remove a tag of yourself from a photo, we will retain a record of that action so that we can block others from tagging you in that same photo.

In addition to these situations, because communication on Facebook is designed to mirror the way communication works in the offline world, you cannot delete certain messages on Facebook that have already been delivered to another person. We describe this in more detail in response to question 7, below.

7. How does Facebook address users who want to delete part of a conversation that happened in conjunction with other users on the site? Describe how shared interactions are treated when requests for deletion are made. What happens when a

user demands the deletion of content created by others because it mentions them, includes their likeness, etc.?

When we build our tools to facilitate social interaction on Facebook, we strive to do so in a way that reflects familiar experiences of social interaction. As a result, as described above, if you send a message to a friend on Facebook, you will keep a copy of the message and send another copy to your friend. If you then delete the message, your friend's copy is not affected. This approach, which we describe in our Help Center, works the same way that Internet email and paper letters do. We believe that deleting your copy of the message, without affecting your friend's copy, best preserves the social expectations people have developed for that kind of communication. It also protects your privacy if you want to be able to store communications that you receive in your Facebook account even if a friend chooses to delete them.

In contrast, sometimes when you communicate more broadly you expect that removing your communication will prevent other people from being able to see it. For example, if you write a message directly on your friend's Wall and then later delete the message, nobody will be able to see it on Facebook after you delete it. Again, this is designed to reflect how people expect public message postings to work: removing a post from a physical bulletin board, for example, causes the post to be unavailable to everyone. As we build new products and features in the future, we'll continue to work to implement removal in a way that is consistent with people's expectations about how communication works in the offline world.

If someone posts information on Facebook that refers to you, we offer a number of options if you have concerns about being mentioned. First, you can choose to remove the post from your profile page, so that visitors to your page won't see it. (You also can choose to review all posts in which you are tagged before those posts can appear in your profile in the first place.) Second, you can choose not to be "tagged" in the post, which removes any links between you and the post.

We also have pioneered an innovative tool called "social reporting" that helps people directly notify others of material they want removed from Facebook, and that gives people more reporting options if they are concerned about material they encounter on Facebook.

For instance, if a friend makes a post about you that you do not like, you can use the social reporting feature to ask that friend to remove it. Because the reporting process is both private and similar to the kind of communication that two people might have in the offline world, it has proven to be a hugely successful system for dispute resolution between the parties involved.

Moreover, social reporting has also proven an extremely effective mechanism to combat bullying and other abusive behavior. Through our social reporting tool, people also have the option to block communication with others, report material that may be in violation of our policies to Facebook for review (and potentially removal), or even send a copy of abusive material to a trusted friend or adult who may be in a position to help address the person's concern.

As an example, if you objected to a photo your friend posted because it was unflattering, you could use the social reporting tool to indicate that you don't like it.

The screenshot shows a dialog box with a blue header containing the title "Is this photo about you or a friend?". Below the header, there are two main sections. The first section is titled "Yes, this photo is about me or a friend:" and contains three radio button options: "I don't like this photo of me" (which is selected and circled in red), "It's harassing me", and "It's harassing a friend". The second section is titled "No, this photo is about something else:" and contains six radio button options: "Spam or scam", "Nudity or pornography", "Graphic violence", "Hate speech or symbol", "Illegal drug use", and "My friend's account might be compromised or hacked". At the bottom left of the dialog, there is a question "Is this your intellectual property?". At the bottom right, there are two buttons: "Continue" and "Cancel".

Next, the social reporting tool would offer options for addressing the problem, such as sending a message to the user who posted the photo to ask her to remove it.

The screenshot shows a dialog box with a blue header containing the title "What You Can Do". Below the header, there are three radio button options: "Message Annie Ta to remove" (which is selected and circled in red), "Unfriend Annie Ta", and "Block Annie Ta". Under the "Message Annie Ta to remove" option, there is a text input field containing the message "Hey, I don't like this photo. Please remove it." Below the input field, there is a note: "You and Annie will no longer be able to see each other or connect on Facebook". At the bottom right of the dialog, there are two buttons: "Continue" and "Cancel".

Depending on the nature of the problem, the tool would present other options, such as contacting an authority figure or friend to help you work out the issue in person. (Where appropriate, of course, you also could report the photo to Facebook directly.)



These tools provide meaningful ways for people to address concerns with information posted about them by others on Facebook. In fact, we believe these tools are more robust than the tools offered on other sites across the Internet to address these types of concerns. We are not aware, for example, of any other site or online service that provides the same infrastructure and mechanisms for resolving disputes or concerns about the shared use of data or the posting of information that can be viewed by others.

As noted above, Facebook is designed around the notion that the same social norms that drive human interaction in society — such as authenticity, friendship, trust and sharing — should exist on our site. Our efforts to promote these social norms help explain why we require that you use your real name on our site. The idea is that if you use your real name, you are more likely to abide by the same principles that drive social interaction in the brick and mortar world — and be held accountable if you do not.

8. First Amendment scholar Eugene Volokh famously described a certain view of privacy as the “right to stop people from talking about you.” How does Facebook empower users to protect their privacy while protecting free speech values?

In the passage referenced above, Eugene Volokh was addressing the tension between the core values of free speech and privacy. As Professor Volokh explains, most people would like to control what others say about them; at the same time, they do not want to be restricted in what they can say about others. We work hard to build our service in a way that promotes free speech while empowering people to protect their own privacy. One way that we do this is to respect traditional social norms, which give people broad freedom to speak and to encourage them to take responsibility for the consequences of their speech.

Unlike many services on the Internet, Facebook is based on a real-name culture, which means that people are required to communicate on Facebook using their real identities. This encourages civil and respectful discourse and makes people accountable for what they say, just as they are in the offline world. It also gives people the ability to use society's existing legal tools where necessary to ensure that accountability. And we've worked hard to create a service that mirrors our society's approach to balancing free speech and privacy offline: allowing people to speak publicly so long as the speech is not unlawful (e.g., a defamatory statement), hateful, or threatening, and offering tools to resolve problems when people disagree with what others are saying. Our decision to build a real-name culture and integrate traditional social norms into Facebook is part of the explanation why our innovative social reporting tool, discussed above, has been so successful. Many people who have concerns about other people's posts are able to resolve their concerns directly, or with the help of another person in their community, just as they would offline.

Another tool to communicate on Facebook while managing your privacy is the unprecedented level of granular control that Facebook provides over how information about you is shared. You can control what information you publish, and curate on an item-by-item basis who can see information you post. Recognizing that each person will have different preferences when it comes to privacy — and that a person's preferences may differ depending on the information itself — we believe that providing individual settings is the best way to give people control over their privacy without stifling the social communication that is the reason they use Facebook in the first place.

Apart from our service itself, we are committed to taking steps to promote individual responsibility and privacy online. That is why we have supported academic research focused on digital citizenship and online safety and privacy. We also partnered with the White House's anti-bullying initiative, offering resources to help teenagers know how to get help with bullying and helping parents learn the signs that they may need to intervene, and we recently teamed up with Time Warner to launch the "Stop Bullying: Speak Up" application on Facebook, which encourages students and adults to take a pledge of responsibility to help stop bullying.

The industry-leading controls that we offer on Facebook are key components to ensuring privacy online. But we believe that our community education and social reporting initiatives are just as critical to promoting a culture of respect online, so that people who use Facebook are empowered to communicate freely while making the privacy decisions that are right for them.

* * *

We hope that this information about our commitment to robust data storage and deletion practices and our ongoing efforts to provide people with control over their information on Facebook is helpful to you. Please let us know if you have any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to be 'Joe Sullivan', written over a horizontal line.

Joe Sullivan
Chief Security Officer