

Filed Under Seal

EXHIBIT M

Document Provided in Native Format

facebook

facebook

Safety on Facebook

Tim Sparapani, Director of Public Policy
NAAG Presidential Initiative Summit
February 8-10, 2010

Agenda

- 1 Mission & Approach to Safety Leadership
- 2 Robust Security Systems and Safety Tools
- 3 Safety Focus Areas
- 4 A Commitment to Collaborate
- 5 Future Safety Innovations

Mission & Approach to Safety Leadership

Our Mission: Give people the power to share and make the world more open and connected

- Building a trusted environment is fundamental to who we are
- We believe – and have always believed – in addressing safety issues proactively

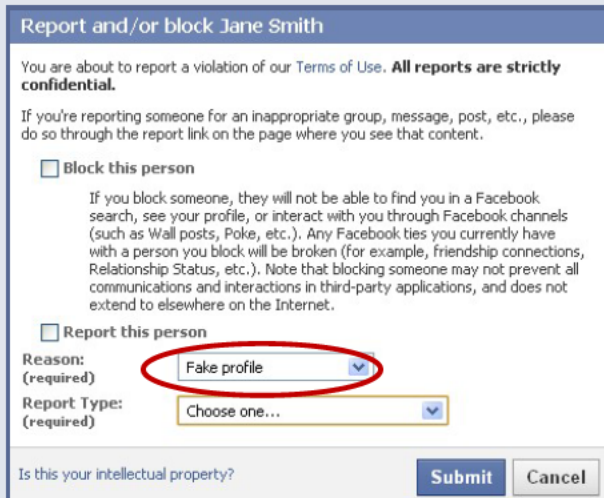


Mission and Approach to Safety Leadership

- Facebook's mission - to give people the power to share and make the world more open and connected - is at the heart of everything we do. Providing a safe and trusted environment where people feel comfortable sharing - and where they have complete control over what they share and with whom they share it - is a core part of this.
- With 400 million people now using Facebook in countries around the world, we of course can't prevent all bad activity. No community this large, whether online or off-line, can. However, by fostering and promoting a real name culture where people are accountable for their actions, building automated systems that flag and block suspicious activity, and working closely with law enforcement to bring perpetrators to justice, we can drastically reduce the number of bad incidents.
- We're proud that even as our user base has grown dramatically over the last six years, through the efforts of our User Operations, Security, Engineering, Policy, and Legal teams, we've managed to maintain a trusted environment that we consider so critical to sharing.

Mission and Approach to Safety Leadership

Focus on real name culture – fake names and hidden identities are incongruous with our mission



Report and/or block Jane Smith

You are about to report a violation of our Terms of Use. All reports are strictly confidential.

If you're reporting someone for an inappropriate group, message, post, etc., please do so through the report link on the page where you see that content.

☐ Block this person

If you block someone, they will not be able to find you in a Facebook search, see your profile, or interact with you through Facebook channels (such as Wall posts, Poke, etc.). Any Facebook ties you currently have with a person you block will be broken (for example, friendship connections, Relationship Status, etc.). Note that blocking someone may not prevent all communications and interactions in third-party applications, and does not extend to elsewhere on the Internet.

☐ Report this person

Reason: (required) **Fake profile**

Report Type: (required) Choose one...

Is this your intellectual property? ☐

- Real people, real relationships
- Monitor name changes, age changes
- Aggressive removal of fake accounts

Mission and Approach to Safety Leadership

-The principal safety issue Facebook works to address is anonymity. While appropriate in some settings, fake names and hidden identities are incongruous with Facebook's goal of allowing people to share and communicate more openly and efficiently. When users are allowed to misrepresent themselves, trust and accountability break down, and people feel less confident in their interactions.

- We only map out the "real" people and real relationships – we have zero economic incentive to help develop non-real relationships. Our advertisers don't want it and neither do our users. We monitor things like age and name changes to determine whether fake accounts exist and when someone switches info, that's a red flag for us.

- We aggressively remove fake accounts and provide resources so that our users know how to report them (through our Help Center).

Robust Security Systems and Safety Tools

These enable us to:

Authenticate

- Social and technical checks at signup
- Ongoing technical and community verification including identity and age

A screenshot of the Facebook sign-up form. It includes fields for First Name (Jane), Last Name (Smith), Your Email (j.smith@email.com), New Password (masked with dots), I am: (Female), and Birthday (Mar 5, 1979). There is a link 'Why do I need to provide this?' and a green 'Sign Up' button.

Promote user control

- Granular privacy settings
- Publisher Privacy Controls
- Special provisions for minors

A screenshot of the Facebook privacy settings menu. It shows options: Everyone, Friends and Networks, Friends of Friends, Only Friends (selected with a radio button), and Customize. There is a 'Share' button and an 'Options' link with a magnifying glass icon.

Robust Security Systems and Tools

Protecting our users has always been a top priority for Facebook. We have devoted significant resources to developing innovative and complex systems and tools to proactively monitor the site and its users for suspicious activity and to allow users greater control over their information. These systems also allow us to combat security threats and respond to abuse.

Authenticate:

- We have technical systems in place to flag and block fake profiles based on name and anomalous site activity. Users who send lots of messages to non-friends, for example, or whose friend requests are rejected at a high rate, are marked as suspect. We've built extensive greylists that prevent users from signing up with names commonly associated with fake accounts. We are committed to making these systems even more robust, which is why we have a team of security experts and site integrity engineers working on these systems and developing new ones.
- For teens, we selectively ask questions when a friend request is sent or received. (i.e. Do you know the person? Do they go to your high school? Are they under 18?).
- We also have systems in place at the point of sign-up to prevent people who identify themselves as under the age of 13 from creating accounts. It's a violation of our Statement of Rights and Responsibilities to provide false birth date information, and we have community verification systems after sign-up to help identify people who are doing this so we can take appropriate action. We also encourage users to report people who have falsified their age either through the report links on the site or through the dedicated contact form in our Help Center.
- We believe that a layered approach to age verification is the most effective. There isn't ONE solution, there is no 'holy grail.'

Promote user control

- Privacy is core to the Facebook experience, and a fundamental element of maintaining personal privacy online is being able to control what one shares and with whom. We offers users industry leading tools to control their information, and regularly remind people to adjust their privacy settings to match their level of comfort and review them often. We also use the Facebook Blog to educate users about privacy. For Data Privacy Day on January 28, for example, we invited experts from around the world to share their perspectives on the meaning of privacy in the digital age and offer advice for managing it online.
- We are constantly offering our users new ways to control their information. For instance, in December we introduced Publisher Privacy Controls that allow users to select who sees any piece of content that they publish. They can make their status updates available to some people (like family members) but not others (like colleagues). This feature was developed in direct response to user feedback.
- We make special provisions for minors' privacy. Settings for minors are always more restrictive than those for adults. If you're a minor, when you share something with "Everyone", it will mean at most friends of friends and members of any school or work networks you've joined. Additionally, minors do not have public search listings created for them, so they do not appear in outside search engines until they have turned 18.

Robust Security Systems and Safety Tools

Combat security threats

- Detect and flag compromised accounts
- Block malicious links from being shared
- Add phishing and malware sites to browser black



Prevent, monitor and respond to abuse

- Robust reporting infrastructure
- Dedicated global team of moderators
- Address hundreds of thousands of user reports weekly
- Use automated systems to disable thousands of accounts weekly

Combat security threats

- Security is a top priority for Facebook, and we devote significant resources to helping our users protect their accounts and information.
- We've built numerous defenses to combat phishing and malware, including complex automated systems that work behind the scenes to detect and flag Facebook accounts that are likely to be compromised (based on anomalous activity like lots of messages sent in a short period of time, or messages with links that are known to be bad).
- Once we detect a phony message, we delete all instances of it across the site. We also block malicious links from being shared and work with third parties to get phishing and malware sites added to browser blacklists or taken down completely. Users who've been affected are put through a remediation process so they can reset their password and take other necessary steps to secure their accounts.
- We also regularly work with others across the industry to identify and respond to potential threats to our users. As an example, on the malware front, we've worked with Microsoft to push a solution to the Koobface virus on user machines through Windows Update. We've also worked with McAfee to integrate a unique Scan and Repair tool into our own remediation process for compromised user accounts and to offer all 400 million Facebook users a complimentary subscription to McAfee security software.
- Security is an arms race, though, and our teams are always working to identify the next threat and build defenses for it. Most of these defenses are invisible to users, and while malicious actors are constantly attacking the site, what you see is actually a very small percentage of what's attempted.
- We work hard to educate people on how to be safe through our blog and the Facebook and Facebook Security Pages. We regularly update the Facebook Security Page and its over one million fans with tips and information about new threats. We also work with outside experts on education initiatives. Example: October blog post with the National Cyber Security Alliance to wrap up National Cyber Security Awareness Month.

- In addition to our automated systems and educational efforts, we have dedicated Security and Legal teams whose responsibility it is to investigate spam, phishing, and malware campaigns and go after the people behind them. A recent example is the judgment we won in the amount of \$711 million against the notorious spammer Sanford Wallace.
- We maintain a strong relationship with security experts around the world and work closely with them in the rare instances in which they find vulnerabilities on Facebook.

Prevent, monitor, and respond to abuse

- We have a robust reporting infrastructure that leverages Facebook's 400 million users to keep an eye out for offensive or potentially dangerous content. This reporting infrastructure includes report links on pages across the Facebook site, systems to prioritize the most serious reports, and a trained team of reviewers who respond to reports and escalate them to law enforcement as needed. The team treats reports of harassing messages as a priority, reviewing and acting on most reports within 24 hours. We also prioritize serious reports submitted through the contact forms in our Help Center.
- Our moderation team is global (US & Dublin) so that we're able to supply 24/7 support to our users.

Safety Focus Areas

Registered sex offenders

- Proactive work with states' AGs to run RSO lists against user base
- Support for Applied Internet Registry Requirement
- Shared removal statistics with NY, CT AGs
- 4000+ accounts disabled in 2009

Child pornography

- Automated tools to prevent the dissemination of URLs
- Collaboration with NCMEC, DOJ
- Dedicated teams to respond to rare instances when child porn is detected

Safety Focus Areas

Preface: only a tiny fraction of users will ever experience the following kinds of behaviors on Facebook. We focus on these areas because we want to ensure that Facebook remains a trusted environment and because we take any threat to our users' safety very seriously.

Registered sex offenders

-We have been working proactively with states' attorneys general to run their lists of registered sex offenders against our user base. Our team uses various internal tools to automatically find matches. Any potential matches are evaluated more fully by our internal team of investigation professionals. If we find that someone on a sex offender registry is a likely match to a user on Facebook, we notify law enforcement and disable the account. In some cases, law enforcement has asked us to leave the accounts active so that they may investigate the user further. We have worked proactively to establish a publicly available national database available to everyone of registered sex offenders that enables real-time checks and includes important unique information like email addresses and IM handles.

- We applaud NY and CT for their Applied Internet Registry Requirement — i.e., they give us the e-mails of the RSOs and we can clean out their accounts if they are on Facebook (this helps us distinguish between people with the same name.) If they have multiple e-mails to share, we'll run them all.

- There's no legal obligation to ban RSOs, but FB voluntarily undertakes this activity.

- When NE tried to ban RSOs from using social networks through statutes a TRO issued by a court prevented their activity.

- We shared our stats on removing RSOs with the AG of CT and AG of NY

- Shut down 4,000 accounts last year

- We've hired a third party to build a separate list from Sentinel. Every state and locality has a different format for their lists. Different info. Different character fonts, etc. We periodically run that list against our user list. We do not wait to be asked to do it.

- We need help getting international lists. We've requested a list from the UK and reached an agreement to have them at least confirm a name of someone who is on a list when a user reports that another user is an RSO.
- The KIDS Act needs to be put into effect. Private companies shouldn't have to pay to get this done; the DOJ should just provide it.

Child pornography

- We use automated tools to 'black hole' every link that contains child pornography so that these links cannot be distributed across the site. We also have a dedicated team that responds to the rare occasions when child pornography is detected on the site. They report every incident immediately to NCMEC and DOJ.
- We need NAAG to help us get the hashlist from DOJ of known kiddie porn links. We are begging for it.

Safety Focus Areas

Suicidal activity

- Special reporting procedures
- Immediate contact with law enforcement
- Partnership with National Suicide Prevention Line
- Resources and FAQs in Help Center

Cyberbullying and harassment

- Founding member of Stop Cyberbullying Coalition
- Aggressive response to reports of harassment (24hrs)
- Educational resources to help users respond to harassment
- Partnerships with MTV, BBC UK, NCPC, and others

Suicidal activity

- The promotion of self-harm, including eating disorders, cutting, etc., is a violation of our Statement of Rights and Responsibilities, and we encourage users to report this content when they encounter it using the links we've provided throughout the site. Our dedicated team of User Operations analysts reviews these reports and disables photos, groups, events, etc. as appropriate. When we receive a report for someone who has posted suicidal content on Facebook, we immediately alert the National Suicide Prevention Lifeline and we encourage the user to contact their local authorities/law enforcement immediately. We've also posted an FAQ to the privacy and safety page in our Help Center with information and links to suicide help resources.
- Facebook helps prevent this kind of behavior on a regular basis. Our real name culture helps people identify those who are truly in need - their friends see and sense the despair and can respond in real time to a cry for help.

Cyberbullying and harassment

- We were a founding member of the Stop Cyberbullying Coalition operated by Parry Aftab and WiredSafety.
- We have a robust reporting infrastructure that leverages Facebook's 400 million users to keep an eye out for offensive or potentially dangerous content. This reporting infrastructure includes report links on pages across the Facebook site, systems to prioritize the most serious reports, and a trained team of reviewers who respond to reports and escalate them to law enforcement as needed. The team treats reports of harassing messages as a priority, reviewing and acting on most reports within 24 hours. We also prioritize serious reports submitted through the contact forms in our Help Center.
- We've produced new FAQs for our Help Center that specifically address how to prevent or respond to cyberbullying. We have also partnered with key organizations like MTV on their 'A Thin Line' campaign to educate young people about the dangers of digital abuse; with the BBC on their 'bullyproof' campaign, and regularly ask guest authors to blog about

cyberbullying on the Facebook Blog, which reaches over 7 million people. The National Crime Prevention Council is a great example of this – they did a blog in October for National Crime Prevention Month in October.

Safety Focus Areas

Missing children and runaways

- Regularly assist law enforcement in investigations
- Triage subpoena workload multiple times daily
- Ensure that IP info that might help locate missing teens is passed on quickly
- Two cases in VA, CA last week alone



Missing children and runaways

– We have been incredibly successful in helping to locate and return missing teens. Law enforcement have been effusive in their praise because we triage our subpoena workload several times a day to find and prioritize these urgent cases to make sure that IP location that might help locate the teen gets to LE quickly.

- Just last week we helped law enforcement in Fairfax, VA and Menlo Park, CA find and return two missing kids.

Extra example:

- Last July, we received a court order requesting IP data and basic user information for a minor who had gone missing. Over the course of the next week, we worked closely with law enforcement over email and by telephone. Ultimately, the minor was found using the exact IP data we had provided. Similarly, a Facebook user went missing in Canada, and a demand for ransom was made. The Royal Canadian Mounted Police contacted us, and we followed our procedure for imminent threats. When a message was sent to a friend from the missing person's account, we provided the necessary data, enabling the RCMP to locate and bring the person to safety.

A Commitment to Collaborate

- Signed agreement with 49 AGs to help protect children from online predators (2008)
- Active participation in Internet Safety Technical Task Force (2009)
- Successful conclusion of two-year agreement with NY AG regarding content review, with 99.99% completion rate (2009)
- Regular interaction with law enforcement

September 17, 2009 4:27 PM PDT

Facebook break leads to burglary suspect

Commitment to Collaborate

- In early 2008, Facebook signed an agreement with 49 Attorneys General to help protect children from online predators and at the end of 2009, the New York Attorney General's office cited Facebook's cooperation in identifying and disabling the accounts of registered sex offenders.
- Facebook also participated in the Internet Safety Technical Task Force, a group of internet businesses, non-profit organizations, academics, and technology experts that worked together to identify effective tools and technologies to create a safer environment on the Internet for youth.
- At the end of 2009, we successfully concluded a two year agreement with the NY AG's office regarding content review. We hit a 99.99% completion rate in terms of hitting our review targets in the agreed-upon time frames.
- Regular interaction with law enforcement:
 - In addition to working with Facebook as a company, many police departments around the world are also using the tools Facebook provides to aide in their work. Literally hundreds of police departments from small towns like Brunswick, Maine to major cities like Philadelphia and Chicago have official pages on Facebook.
 - The ways these departments are using Facebook vary. Some are using it simply as a way to update the community. Others use Facebook as a way to promote the work they've done. The most innovative departments actually rely on Facebook to solve crimes, including crimes involving children.
 - One great example comes from Toronto where a law enforcement organization called Toronto Crime Stoppers is using its Page, as well as Facebook groups and events, to inform Toronto residents about crimes in their area and encourage them to provide anonymous tips. On Facebook, messages can be broadcast quickly and easily to wide audiences across a big city like Toronto and then receive immediate feedback. Outreach through Facebook has helped Toronto Crime Stoppers sniff out threats against local schools, bring much

needed help to people at risk of committing suicide, warn the public about criminals on the loose, and locate missing persons.

A Commitment to Collaborate

- Memberships in key safety organizations
- Campaigns to raise awareness about Internet safety
- Proactive creation of global Safety Advisory Board
- Regular blog posts on safety (reach 7m+ users)



Commitment to collaborate

-We know that the best way to protect our users and promote a safe environment is to work with others towards this goal. We welcome the opportunity to work with people in this room.

- We've teamed up with a wide variety of groups to address safety. This past year, we joined the Family Online Safety Institute as a member, and we recently became a member of the Internet Watch Foundation. We've also worked with groups like MTV, the BBC, the National Crime Prevention Council and WiredSafety on educational initiatives related to cyberbullying and digital abuse.

- The latest step in our commitment to improve safety on Facebook and across the Internet was the formation of our global Safety Advisory Board in December. This board is comprised of five leading Internet safety organizations from North America and Europe that serve in a consultative capacity to the company on issues related to online safety. The five organizations on the board are Common Sense Media, Connect Safely, WiredSafety, Childnet International and The Family Online Safety Institute (FOSI).

- We continue to ask safety experts from around the world to blog about safety for our users on the Facebook Blog, which reaches over 7 million people.

Future Safety Innovations

- Brand new safety page in Help Center for March 2010 (facebook.com/safety)
- Development of new educational resources for parents, educators, teens and law enforcement
- New ways of using the Facebook platform to respond to emergencies
- **Safety is part of our innovation cycle**

Future Safety Innovations; our asks; closing

- We are in the process of creating a new safety page for Facebook's Help Center to make our safety resources even more useful to our users - especially as the site grows. The Safety Advisory Board will be advising us on this project and we are thrilled to have their valuable input.
- As Facebook has grown, we've become more aware of providing audience-specific safety resources for our users. We're proactively working to build out the safety page of our Help Center to create even more useful content for audiences like parents, educators, teens, and law enforcement.
- In addition to addressing personal safety on Facebook, tragedies like the recent earthquake in Haiti remind us that Facebook can be used as a platform to promote public safety, including emergency response and disaster relief. We created the 'Global Disaster Relief' page on Facebook directly after the Haiti earthquake and watched as this page grew to 240,000+ members in a matter of days. We used this page to highlight the ways that people could donate to earthquake relief, and asked Pres. Bush and Pres. Clinton to film videos for our users highlighting the importance of helping in Haiti. We plan to use this page to respond to future emergencies when they occur.
- We think Facebook is an ideal platform for emergency response – from events like the Haiti earthquake to helping to find missing children -- so expect to hear more about this in the coming months. (Probably shouldn't mention NCMEC by name – they told us DOJ doesn't allow any sort of announcement until agreement is finalized.)

Our asks

- We need a national database of convicted sex offenders that includes online identifiers like email addresses and IM handles, and that's accessible to companies that are concerned with keeping sex offenders off their networks. We actively supported passage of the KIDS Act, which will create just such a database, and were glad to see it signed into law last fall, but the Act needs to be implemented now, not two years down the road.
- We need internet companies to have access to hashes of known child pornography images. Facebook is now the largest photo-sharing site on the web, with over a billion photos uploaded every month. We report instances of child pornography to the National Center for Missing and Exploited Children when they're found by us or by our users. With

better technology, however, we can block them upfront and identify the people responsible so we can preserve information and notify law enforcement as quickly as possible.

- We need a renewed investment in youth internet education programs. We've worked closely with private organizations on various safety and security curricula, but a mandatory program taught at schools around the country and aimed at teaching kids the rules of the road would drastically reduce the number of bad incidents.

Closing

- Protecting children is a responsibly shared by parents, teachers, children themselves, websites, education organizations, and law enforcement, and we plan to continue our diligent work with all of these groups to build a safer Internet.

- Safety as part of innovation cycle – we will never stop thinking about the safety of our users, and will continue to develop new tools and partnerships to promote a safe and trusted environment.

facebook

(c) 2009 Facebook, Inc. or its licensors. "Facebook" is a registered trademark of Facebook, Inc. All rights reserved. 1.0