# EXHIBIT K

(computers) I say listen to 13 year olds! I think many would be surprised at their mature approach to life.

Every day our rights are being boxed up and shipped to byte heaven - for our own safety - so they say. Our emails are scanned, sorted, and labeled. Our Internet travels are monitored, and when we buy something with plastic, ask for air miles, or use a customer discount card, we are recorded and the info used to make sure they eventually we get an ad in our face and our habits sold to marketeers. Do we assume the governments haven't considered using that information to monitor our movements, buying habits, and how much we spend and on what - for our own safety?

Facebook is helping to lead the way in protecting children on social networks. It is also helping to lead the way to where any company can read 'personal' data, and based on the communication, make an assumption.

The youth of today are becoming complacent to being 'monitored' and are more likely to accept Big Bro watching their every move. Next, as Leonard Cohen would say, is ".. a camera in the bedrooms of the poor."

No matter where the predator hides, and under what guise, it is still up to the parents to get educated, have a good sit-down with their kids at a early age, and not be afraid to tell it like it is. Talk about the predator and how they might work, what could happen yadda yadda... What the parent forgets, the kids get off the TV, at school, on the 'net, from friends anyway.

Bottom line, get use to being monitored, be careful what you discuss lest you raise a flag - - maybe this post will, and parents - reinforce what they are taught at school - - educate your kids!

I am glad they caught what they alleged to be a child predator, but wonder if at the expense of privacy could not have been conducted without affecting others privacy.

i

0 0 Rate This

Reply

**Richard** · 982 days ago

Shouldn't that be "Big Blud"? :o)

0 0 Rate This

Reply

**Sum Guy** · 982 days ago

There are good reasons to lose privacy, as in this case, but there are cons to this software too.

I think all children's communications should be monitored this way, but adult communications should remain private unless communicating with a minor. There are many sick people out there. If all minors are monitored it pretty much guarantees more pedophiles will be caught. I am sure some will slip though, but it seems like a good idea.

There are a lot of things that adults talk about that is illegal. Drugs and protest to name a few. I think what one does to him or her self is their choice. As long as alcohol is legal I think enforcing drugs is hypocritical.

Our children need to be monitored, The misbehave in way that would shock most of us when we are not looking. This current generation or adults is pretty poorly mannered. monitoring them may help the quality of the next generation to become important adults.
Of course this wont fix our society but maybe it will increase the good to bad ratio.

0 1 Rate This

Rate This

Reply

**Ken** · 982 days ago

Let's look at this from another perspective. Since you are unwilling to educate and monitor your own children, you decide to pass this job off to someone else to do. What if the person that is monitoring your children is a child predator? You would then have to monitor the monitors. What if a child predator was able to get a hold of the logs for your monitored child? That would give them vast more information on your child and their habits to allow your children to be social engineered that much better.

What about another scenario; What if your child joked about bombing some place? Or became mad at someone and wished them dead? By monitoring everything they do, day in and day out, I am sure that something your child has said could be construed as illegal, or classified as terrorism. I can see the headline now, "11 year old arrested. Science project classified as a WMD". Or an online psychological evaluation deems your child is a threat to society and they are put into an institution ("I'm sorry Ma'am we can't risk another Ted Bundy")

I reiterate, educate your children, and leave my American freedoms alone.

2 0 Rate This

Reply

**Tony** · 981 days ago

"[A] low false-positive rate has the serious downside of letting many dangerous communications go through unflagged."

As opposed to other communications media such as email, IM, texting, phone calls, snail mail or even good old face-to-face encounters -- all of which let 100% of communications go through, even if dangerous or illegal. It's easy to lose sight of that in the rush to hold new technologies to a higher standard.

0 0 Rate This

Reply

**oncefallendotcom** · 980 days ago

When we allow one group to be targeted, we allow all groups to be targeted. We are growing to accept big brother surveillance.

2 0 Rate This

Reply

**Maxwell** · 956 days ago

This is another reason why i feel like I'm different to everyone else, is it really SO hard to stay safe online I'm 13 and I have never let any stranger be my friend or talk to me.

Most of them are idiots for even letting a stranger even talk to them let alone actually talking back to them, Our schools really should try to teach them how to be safe online better.

Rate This

0 1 Rate This

Reply

**About the author**

I've been writing about technology, careers, science and health since 1995. I rose to the lofty heights of Executive Editor for eWEEK, popped out with the 2008 crash, joined the freelancer economy, and am still writing for my beloved peeps at places like Sophos's Naked Security, CIO Mag, ComputerWorld, PC Mag, IT Expert Voice, Software Quality Connection, Time, and the US and British editions of HP's Input/Output. I respond to cash and spicy sites, so don't be shy.

View all posts by Lisa Vaas

About Naked Security About Sophos Our Authors Awards Got a story for us?

Tags

Adobe Android anonymous Apple data breach data loss DDoS Encryption Exploit Facebook General Google hacking iPhone IT Malware Microsoft password Patch Patch Tuesday phishing Privacy Scam Spam Twitter Video vulnerability web web 2.0 www

Categories

Android (1,187) Botnet (545) Celebrities (623) Cryptography (1,588) Denial of Service (767) Fake antivirus (110) Firefox (468) Google (2,382) Hacked (277) Internet Explorer (693) Java (361) Malware (6,281) Mobile (1,565) Nude Celebrities (229) Operating Systems (72) OS X (665) Phishing (864) Podcast (941) Ransomware (396) SophosLabs (2,035) Technologies (37) Video (965) Web Browsers (415) Windows (882) Windows phone (116)

Archives by month

March 2015 (100)
February 2015 (108)
January 2015 (109)
December 2014 (90)
November 2014 (87)
October 2014 (94)
September 2014 (93)
August 2014 (90)
July 2014 (104)
June 2014 (97)
May 2014 (101)
April 2014 (96)
March 2014 (96)
February 2014 (86)
More

Download some free tools

**Free anti-virus for your Mac**
Free antivirus that works simply and beautifully

**Free Android protection**
Free antivirus for all your Android devices

More free tools

Take a look at our products

Endpoint Mobile Email
Encryption Network Web

Try out our free trials and demos

Investigate the threats

Virus and spyware analyses
Threat Center
Inside SophosLabs

SecurityWatch *with Neil Rubenking*

Search Security Watch

Top Categories

SEE ALL »

Trending Tags

malware
vulnerability
antivirus
patch
Android
firefox
Apple

SEE ALL »

Follow

More Blogs

AppScout

'Lord of the Rings: Legends' Begins Its Quest on iOS, Android

Forward Thinking

Living With a Sturdy Samsung Galaxy Tab Active

# Facebook Scans Chats for Criminal Activity

Jul 13, 2012 6:00 PM EST | 2 Comments

By Fahmida Y. Rashid

family

sorry i missed the birthday party!

the kids look great 🙂

glad you posted these -- looking forward to seeing more

nice pics, daniel!

family

Social networking is a great way to keep in touch with friends and meet new people. But it's also important to be vigilant about what you say to people you meet online.

Facebook has technology in place to monitor user conversations for suspicious activity and notify police when necessary, Reuters reported yesterday. The scanning technology monitors chats for words or phrases that may signal that something is wrong, such as personal information being exchanged or explicit language being used.

"We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate," Facebook told Reuters.

Facebook security employees don't see any of the conversations until the scanning technology actually flags the exchange. The employees then review the chat to determine whether the police should be notified.

"I find the news to be both scary and more than a bit surprising," Chester Wisniewski, senior security advisor at Sophos, told *Security Watch*. Most communication providers tend to take the stance that since they don't monitor user activity, under the Safe Harbor provisions it isn't their fault if users do something illegal, Wisniewski said.

"If you begin analyzing content, you may be held liable for not stopping something dangerous that traverses your network," Wisniewski said.

### Protect Yourself

While it's nice to know that Facebook is keeping a distant eye on chat logs for criminal behavior, users should exercise some Internet smarts when online. And while we are picking on Facebook a bit, these tips apply to other social networking sites, as well.

- Friending Strangers – Study after study have shown Facebook users accept friend requests from people they don't know. It's easy to lie on a profile, and criminals do it all the time on social networking sites. Sexual predators have pretended to be teenagers to talk to younger users on social networking sites. In a recent analysis, researchers from Barracuda Networks found several fake Facebook profiles using the exact same photograph of an attractive woman as the main profile picture. Once a fake profile is added as a friend, that scammer has access to a tremendous amount of personal data. Screen them out beforehand.

- Chatty Profiles – Many people still have not locked down their social networking profiles, letting people they don't know see their home address, phone numbers, and all other information. If it's that critical to have that much information about you on your profile, at least lock it so that only friends can see it (and then be careful about who you friend…)
- Know About Privacy – Some information, such as login credentials and personal identifying information, should never be shared, even with best friends. Learn how to use the site's privacy controls. Google+ has done a good job of giving users control over who can see their profile data, and Facebook is steadily improving.

"The bottom line is no one should expect any sort of privacy on social networks and these types of programs just further prove that point," Wisniewski said.

**Crimes Against Minors Online Rare**

Facebook relying on software to pre-scan chats protects the company from privacy concerns that someone is monitoring all conversations. But it also means that a lot of other suspicious incidents may be missed.

"I feel for every one we arrest, ten others get through the system," Special Agent Supervisor Jeffrey Duncan of the Florida Department of Law Enforcement told Reuters.

However, before anyone panics, it's worth noting that that Internet-related sex crimes against children are rare. The National Center for Missing and Exploited Children processed 3,638 report of online "enticement" of children by adults last year, 10 percent less than 2010.

Most sex crimes against children are committed by people the children know, rather than strangers. Reuters reported Facebook's technology is more likely to likely scrutinize conversations between two users who aren't already "well-established" in the Facebook universe as friends. In which case, those chats with non-strangers may never even be flagged.

**Protect Children**

Despite the fact that strangers approaching children online is rare, many parents are still jittery. A recent survey of 1,000 parents by MinorMonitor found that 74 percent of parents were concerned about their child's safety on Facebook, with 56 percent worrying about predators.

There are a number of tools available that parents can use to monitor their children's social networking activities. PCMag gave an Editors' Choice award to Socialshield, which lets parents monitor their children's Facebook, MySpace, Twitter, Google+, and Formspring accounts. ZoneAlarm's SocialGuard detects cyberbullying, account hacking, bad links, age-inappropriate relationships, and contact by strangers. MinorMonitor also tracks the child's Facebook activity and sends parents alerts for potential problems.

**Categories:** Security, Privacy
**Tags:** social networking, Facebook, cybersecurity, social network

Tweet 0

- St

**Comments**
blog comments powered by Disqus

| ABOUT | CONNECT | ZIFF DAVIS SITES | SUBSCRIBE | SOCIAL |
|---|---|---|---|---|
| About Us | Login | AskMen | PC/Mac | Facebook |

# Facebook's Spying On You For a Good Cause

Written by **ADAM ESTES**

July 13, 2012 // 01:10 PM EST

Whether you realize it or not, a bundle of sophisticated technology isconstantly scanning through Facebook interactions — wall posts, messages, chats — looking for sexual predators. A combination of intelligent software and human moderators can spot when a predator goes after an underage user and notify police almost in real time as the conversation is happening. The tools pull clues from users' mutual friends, past interactions and age difference to spot potentially abusive conversations and compare them against archives of past interactions that have lead to assaults.

It's part of an aggressive effort the social network has made over the past few years to protect the safety of its 13- to 18-year-old users, and few would argue that the stated goals of the program aren't sound. Nobody likes pedophiles. And nobody wants them picking up kids on Facebook.

Still, there's something unnerving about Facebook reading your messages, isn't there? Preventing crime is one thing, but surveilling the most intimate user behavior is something completely different. At face value, it treats every Facebook user like a sexual predator. Facebook is obviously aware of the privacy concerns and insist that their technology only spots the bad guys. "We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate," the company's chief security officer Joe Sullivan told Reuters this week. Nevertheless, authorities say that existing systems are still inadequate for keeping pedophiles away from minors online. Said one special agent from Florida, "I feel for every one we arrest, ten others get through the system."

From the other side of the fence, though, it's easy to think of Facebook's anti-pedophile software as just another form of moderation. After all, Facebook employs an army of moderators to keep illicit photos from being uploaded, abusive language from being used in the comments and general trollishness from ruining others' experience on the site. What more despicable trolls could there be than pedophiles looking for some underage kids to hit on? The vast majority of the scanning is also algorithmic, so it's not like you have a bunch of Facebook employees poring over your every word. In truth, it's a machine that's trying to spot patterns and red flags. And don't forget: it's for a good cause.

## CONNECTIONS:

- Anonymous Starts Its Own 'To Catch a Predator'
- Internet Eyes Review: Being an Armchair Vigilante Sucks
- Sorry FBI, There Are Probably No Drug Cartels In Second Life

**TOPICS:** facebook, privacy, sexual predators, privacy-and-security

OpenNet Initiative

Search

HOME ABOUT ONI ABOUT FILTERING RESEARCH NEWS BLOG

# Facebook uses scanning technologies, alerts authorites about content

By: Cale Guthrie Weissman on 16 July 2012
Posted in Arrests and legal action, Internet tools filtering, Surveillance, United States of America, United States/Canada

In March of this year, authorities in south Florida arrested a man in his thirties who had used Facebook to make plans to meet up with a minor. According to Reuters, a program designed by the social networking platform to monitor suspicious communications between adults and minors led to the arrest. Facebook regularly scans user content for criminal activity, but the monitoring program is something the social media giant has generally kept quiet about. Reuters explains, "Facebook generally avoids discussing its safety practices to discourage scare stories."

Though often hidden from view, this monitoring program is one of the most advanced of its kind. CNET describes the general mechanics of the program:

> Facebook's software focuses on conversations between members who have a loose relationship on the social network. For example, if two users aren't friends, only recently became friends, have no mutual friends, interact with each other very little, have a significant age difference, and/or are located far from each other, the tool pays particular attention.
>
> The scanning program looks for certain phrases found in previously obtained chat records from criminals, including sexual predators.... The relationship analysis and phrase material have to add up before a Facebook employee actually looks at communications and makes the final decision of whether to ping the authorities.

According to Reuters, this sort of scanning is commonplace for platforms like Facebook—most large social media companies scan chats for inappropriate language and exchange of personal information. However, many social media platforms--especially those tailored for younger audiences--walk a tightrope between utilizing these tactics to safeguard against illegal activity and providing a less restrictive social media platform that will engage users. Reuters explains:

> From a business perspective, however, there are powerful reasons not to be so restrictive, starting with teen expectations of more freedom of expression as they age. If they don't find it on one site, they will somewhere else.

Scanning users' content is not new terrain for Facebook. In April a document leaked showing the kinds of user information Facebook releases to authorities when subpoenaed. While the document provoked public backlash, Facebook is clear about what it does with users' information in the "Information for Law Enforcement Authorities" section of its website.

Facebook acknowledges the difficulties inherent in monitoring content on its platform for criminal activity. Facebook's Chief Security Officer Joe Sullivan, speaking to Reuters, explains, "We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate." Digital Trends explains that Facebook takes active measures to limit communication between minors and unfamiliar adults on its site. Examples include not listing minors within the Facebook search tool and allowing only direct friends of minors into a direct chat. It then scans communications that do take place for keywords and patterns derived from an analysis of chat logs taken from prior criminal cases in order to identify possible threats.

Scanning technologies of this design are just beginning to come to the forefront for various websites. While some sites are reticent to embrace them fully, fearing revenue loss, this example highlights the tactics used and suggests a possible upward trend in surveillance by social media platforms.

## Post new comment

Your name: *

Anonymous

CONNECT WITH ONI

Blog Feed
ONI Newsreel
@OpenNet
ONI on Facebook

OUTSIDE LINKS

Bruce Schneier
CyberLaw Blog
DigiActive
Ethan Zuckerman
Foreign Policy: Net Effect
Global Voices Advocacy
Global Voices Online
Info/Law
Information Warfare Monitor
Infowar Monitor Blog
Internet & Democracy
Jillian C. York
John Palfrey
Jonathan Zittrain
Nart Villeneuve
PolicyBeta - Digital Policy in Progress
Rebecca MacKinnon
Ron Deibert
Sami Ben Gharbia
Somebody Think Of The Children
Surveill@nce St@te

HELP REPORT CENSORSHIP

HERDICTWEB

Suspect a website is being censored? Let us know by reporting it to Herdict!

**E-mail:** *

The content of this field is kept private and will not be shown publicly.

**Homepage:**

**Subject:**

**Comment:** *

- Web page addresses and e-mail addresses turn into links automatically.
- Use [fn]...[/fn] (or <fn>...</fn>) to insert automatically numbered footnotes.
- Allowed HTML tags: <a> <em> <strong> <cite> <code> <ul> <ol> <li> <dl> <dt> <dd> <sup> <h1> <h2> <h3>
- Lines and paragraphs break automatically.

More information about formatting options

CAPTCHA

This question helps to reduce spam on the site. If you need new words, click the double-arrow icon on the form. If you need spoken word, click the speaker.

Type the text

Privacy & Terms

Preview

Harvard Toronto SecDev Group

# Did you know that Facebook monitors postings and chats for sexual predators?

## The social media giant uses monitoring software that can scan and flag suspicious messages to minors from potential predators.

BY MICHAEL WALSH

NEW YORK DAILY NEWS Monday, July 16, 2012, 1:46 PM

A A A

69 3 7

**On March 9th of this year, Facebook noticed suspicious conversations between a man in his early thirties and a 13-year old girl from South Florida.It was reported to authorities and the man was charged.**

Would you want Facebook spying on your conversation? Maybe not, but the social media giant is, in fact, doing such data monitoring now, and is walking the fine legal line in order to help authorities catch sexual predators.

At present, the emphasis is on what are called “innappropriate conversations.” This little-known effort, in fact, has already helped law enforcement officials thwart pedophiles and other sexual aggressors.

For example, Special Agent Supervisor Jeffrey Duncan of the Florida Department of Law Enforcement has witnessed this software work firsthand. On March 9th of this year, Facebook noticed suspicious conversations between a man in his early thirties and a 13-year old girl from South Florida. When the software noticed the sexually explicit nature of the conversations and plans for an encounter after her middle-school classes, the conversation was flagged.

Facebook employees then read the conversation and immediately informed the police. Duncan explained to Reuters that the authorities took control of the girl's computer and arrested the man the next day. The alleged pedophile subsequently pleaded not guilty to the charge of soliciting a minor.

While it worked in this case, the surveillance practice is fraught with legal complexity, and both the company and authorites know it. Facebook tends to avoid comment on this practice, because the organization doesn't want to create scare stories or stir surveillance paranoia.

One way to address such fears is by the use of carefully tuned automatic monitoring software. Facebook's Chief Security Officer Joe Sullivan told Reuters, "We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate."

But keeping false-positive rates low requires certain conversations to go unchecked. When discussing tips from Facebook and similar groups, Duncan said, "I feel for every one we arrest, ten others get through the system."

To minimize the risk of inappropriate surveillance the software and procedures are designed to err on the side of monitoring caution. The software analyzes suspicious sexual conversations between unlikely couples, such as people of drastically different ages. It then uses records of online chats from convicted predators to know what to flag.

*mwalsh@nydailynews.com*

JULY 13, 2012, 2:56 PM

# Facebook scans conversations for criminal activity

**By Walter Pacheco, Orlando Sentinel**

Facebook is scanning users' chats and posts for possible criminal activity, a report from Reuters shows.

The social network's Chief Security Officer Joe Sullivan told the news agency that Facebook monitors conversations for words and phrases that suggest potential criminal activity, as well as the exchange of personal information between users with a wide age gap.

Conversations between users who do not have a well-established history of chatting are more closely watched than others. Facebook's software also searches for words often found in the chat records of convicted criminals, including sex offenders, who used social media to find their victims.

If criminal activity is suspected, Facebook officials notify law enforcement.

The nearly 1 billion member social network has indicated in the past that they work with law enforcement officials when the safety of their users is at risk.

Detectives at law enforcement agencies in Central Florida, including theOrange County Sheriff's Officeand Orlando Police Department, often scan through suspects' social media accounts on Facebook and Twitter for criminal activity.

YouTube is often monitored by these agencies. In the past, agencies have captured gang members who posted short videos of their gang activity.

theguardian

# Facebook puts faith in its software smarts to see off sexual predators

Leading social network argues that it prefers quiet use of sophisticated algorithms over public deterrents

**Jemima Kiss**

Thursday 15 April 2010 21.19 EDT

Facebook has developed sophisticated algorithms to monitor its users and detect inappropriate and predatory behaviour, bolstering its latest raft of initiatives to improve the safety of its users.

Having launched an education campaign, an improved reporting procedure and a 24/7 police hotline on Monday, Facebook told the Guardian that it has introduced a number of algorithms that track the behaviour of its users and flag up suspicious activity, including members with a significant number of declined friend requests and those with a high proportion of contacts of one gender.

Another filter, common on web publishing sites, scans photo uploads for skin tones and blocks problem images - the "no nipples" filter that caused pictures of breastfeeding mothers to be inadvertently flagged and removed by the site last year.

Facebook is the world's largest social network, with 400 million users a month, and employs 1,200 staff including a significant development team: its mainstream success can largely be attributed to its technical prowess. It believes that "under the radar" security systems developed with these engineering skills are more effective than public deterrents.

Facebook's international law enforcement is lead by Max Kelly, a former FBI agent who worked on cyber-crime and counter-terrorism before moving to Facebook five years ago.

Kelly explained that the site analyses users' actions and compares that behaviour to a average set of actions. "The site makes an assessment about that behaviour and if it is too far from normal mode, will degrade the user's experience. So if they are sending too many messages, the site might present a warning or show some captchas [the distorted text which a human can read but a computer can't]."

Persistently aggressive behaviour, or pursuing particular types of contacts such as young women, would be handled by a review team, with some users eventually blocked. Serious offences such as child porn would be removed and the user banned immediately, said Kelly, who described the site's own user base as "the secret weapon" in monitoring and reporting much of the inappropriate behaviour.

In the US, where Facebook's relationship with law enforcement is more established, the site responds to investigations by providing information about, for example, a suspect's location. It has called for a UK equivalent to its partnership with government in the US, which gives it access to data on sex offenders to help identify them on the site. In cases involving children, information and material will be passed to the US National Center for Missing and Exploited Children. Though the centre has links to its UK equivalent, the Child Exploitation and Online Protection Centre, or Ceop, Kelly admitted the procedure needs to be improved.

"If they tell us the user is in the UK, that data goes to Ceop. We have had several meetings with [Ceop chief executive Jim] Gamble but that relationship is not working well," he said, adding that the UK needed a dual reporting system.

Kelly added that the site had to balance its duty to respect its users while meeting its legal obligations, but emphasised that it "only shares data with very good reason".

"If the warrant relates to the location or certain data about a witness or suspect, the team won't dump all the data on that user," he said. "It's not our data to share. The corporate philosophy about data is that the user is in control, and they choose how to share and distribute it. If we are presented with a legal situation where we have to disclose data to law enforcement, the philosophy is to provide the minimum amount of data required."

Media coverage of the site's safety procedures have largely focused on the rift with Ceop over Facebook's refusal to introduce a "panic button" - a logo linking to Ceop - as a deterrent. Ceop's head of safeguarding and child protection, Dr Zoe Hilton, characterised talks as "robust" but said the agency's primary concern was that Facebook did not appear to be passing on reports of grooming and inappropriate contact.

"There is absolutely no legal barrier that would stop a US company passing reports of day-to-day grooming of children to the UK," she said. "They have internet experts managing and assessing risks to children - we have social workers and police. We want a better dialogue on all aspects of their safety, and underage users should be one of those things."

From Ceop's perspective, use of a branded button on popular websites is an important part of a wider campaign to unify safety reporting procedures. Following an education campaign in UK schools, it claims that 5.2m children now recognise the Ceop name and logo. With MySpace and Bebo on the decline, the cooperation of Facebook is essential. Recent research by Ofcom found that a quarter of children aged eight to 12 had profiles on social networking sites, even though most require users to be 13 or over. Though Hilton welcomed Facebook's technical methods of monitoring suspicious user behaviour, she said they were not new and not a substitute for clear reporting.

Ceop had received 253 reports of grooming on Facebook in the first quarter of this year, she said, and 75% of those had come through the Ceop site. "That means those people had to leave Facebook, find our site and then click through 'report a concern', and that's too many stages."

She denied that Ceop was struggling to deal with the volume of reports, and invited Facebook's team to Ceop to see how they manage their caseload. In the long term, she emphasised, Facebook and Ceop needed to have a "strong and warm relationship" and that ideally, a member of Facebook's safety team would be embedded with Ceop to inform its work across education, new technologies and investigations.

Privacy campaigner Christina Zaba said Facebook needed to do more to stop persistent stalkers and bullies who could use multiple identities, and cautioned against the automated profiling of users. Flagging users with too many friends of one sex could penalise gay people or those organising groups such as the Girl Guides, she argued, while users with many declined friend requests could be PRs, campaigners or journalists trying to reach a new audience.

"There are many human variables that are too complex to be monitored in this way," Zaba said. "I'd be happier if the lines of reporting were clearer, and if concerned users could speak to a real person."

Facebook's rival MySpace does not carry the Ceop logo, while Bebo, whose members are generally younger than Facebook's, includes a small Ceop logo on every profile. The branded links have significantly increased the number of reports being sent to Ceop since they were introduced.

More news

## Topics

Facebook
Internet
Child protection
Children
Social networking

More…

# Nowhere to hide: Facebook monitors your chats

JULY 13, 2012

by Chi Ibe

Reports have revealed that Facebook and other social platforms are watching users' chats. The excuse is that it's doing so to monitor criminal activity and notifying police if any suspicious behaviour is detected but what ever happened to good old privacy?

A number of social networking sites have set up a screening process which works by a scanning software that monitors chats for words or phrases that signal something might be amiss, such as an exchange of personal information or vulgar language.

The software pays more attention to chats between users who don't already have a well-established connection on the site and whose profile data indicate something may be wrong, such as a wide age gap. The scanning program is also "smart" — it's taught to keep an eye out for certain phrases found in the previously obtained chat records from criminals including sexual predators.

If the scanning software flags a suspicious chat exchange, it notifies Facebook security employees, who can then determine if police should be notified.

Some critics of this method have suggested that keeping most of the scanned chats out of the eyes of Facebook employees who could compromise the data may help Facebook deflect criticism from privacy advocates, but whether the scanned chats are deleted or stored permanently is yet unknown.

According to Facebook's chief security officer, Joe Sullivan, at least one alleged child predator has been brought to trial directly as a result of Facebook's chat scanning, *Reuters* report.

Facebook works with law enforcement "where appropriate and to the extent required by law to ensure the safety of the people who use Facebook," according to a page on its site.

"We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards.

"We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities."

# Facebook Monitors Potentially Illegal Posts, Chats

***The social media giant scans conversations and posts for potential illegal activity. Should they be found questionable, Facebook representatives reach out to police.***

By **JUSTIN REYNOLDS** (Open Post)
July 13, 2012

Share

Using data recognition software, Facebook employees monitor certain users' posts and chats, scanning them for potentially illegal activity which in some cases has led the social media giant to contact police, CNET reports.

In March, according to a report in Reuters, Facebook software detected that a man in his 30s was talking about sex with a 13-year-old Florida girl and the two planned to meet up after she got out of middle school the following day. Representatives from the company then contacted police, who arrested the man before the meeting occurred.

According to the report on CNET, the company isn't actively monitoring all communications on Facebook, as it wants its users to maintain their privacy. The software the company uses to analyze communications which are potentially illegal has a low false-positive rate, Chief Security Officer Joe Sullivan told Reuters. CNET reports:

> Facebook's software focuses on conversations between members who have a loose relationship on the social network. For example, if two users aren't friends, only recently became friends, have no mutual friends, interact with each other very little, have a significant age difference, and/or are located far from each other, the tool pays particular attention.
>
> The scanning program looks for certain phrases found in previously obtained chat records from criminals, including sexual predators (because of the Reuters story, we know of at least one alleged child predator who is being brought before the courts as a direct result of Facebook's chat scanning). The relationship analysis and phrase material have to add up before a Facebook employee actually looks at communications and makes the final decision of whether to ping the authorities.

For more information on Facebook's privacy settings, click here.

# Facebook monitoring user chats, reporting to police

POSTED BY TIM BUKHER ON JULY 13, 2012 POSTED IN INTERNET LAW & PRIVACY

According to a report via Mashable, Facebook does more than passively scan user profile settings for targeted advertising, it also monitors chats between users for potential criminal activity:

Facebook and other social platforms are watching users' chats for criminal activity and notifying police if any suspicious behavior is detected, according to a report.

…

The software pays more attention to chats between users who don't already have a well-established connection on the site and whose profile data indicate something may be wrong, such as a wide age gap. The scanning program is also "smart" — it's taught to keep an eye out for certain phrases found in the previously obtained chat records from criminals including sexual predators.

If this is true, Facebook may be facing some serious class action litigation soon. In fact, I was so surprised by these allegations and their potential legal exposure to Facebook, I immediately scoured Facebook's privacy policy to see if they had hidden some sort of "out" for themselves with regard to what information they share about you. The only clause I found anywhere nearing this was:

We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you.

We can probably assume that the authorities are not advertising partners or customers, but since the policy makes no mention of the authorities, then the above is probably the closest Facebook gets to having a policy with regard to the information it shares about you. That said, I do not see a police report "removing" the name of the reported party.

The Facebook Help center does explain how Facebook shares certain information with the authorities:

We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.

Of course I had to go looking for the Help center to find this information, so I cannot imagine that it would fall under the honest disclosure of a readily available privacy policy. We'll see how this develops.

MyFoxTampaBay.com 78° Broken Clouds DOWNLOAD IT NOW! ● Web Search...

# Facebook uses technology to spy on private chats

Posted: Jul 13, 2012 8:00 AM CDT
Updated: Sep 07, 2012 8:00 AM CDT

By: FOX 13 Tampa Bay Staff CONNECT

TAMPA (FOX 13) - A debate between privacy and protection is heating up again, and Facebook is front and center.

It's no secret the stuff you post publically online can be monitored, but your private chats, too? According to Reuters, the answer is yes.

Facebook's chief security officer admits Facebook users are being monitored for any suspected criminal activity, and it's not just the stuff you post on timelines.

Using software, the company says it's monitoring personal chats as well. Using smart software, Facebook scans those chats for certain phrases, exchanges of personal information and vulgar language.

If it sees something suspicious, it flags it, and only then would an actual person read it. At that point, a security team takes over, reads the chat and then contacts police if needed.

Facebook says the technology has a very low false-positive rate to protect its users' privacy, but as expected there has been backlash from users. Some feel their private conversations are being violated.

But the company points to one instance where the technology helped net an alleged sexual predator: The software red-flagged a man's chat with a 13-year-old girl in South Florida.

In the conversation, authorities said he was making plans to meet with her after school. It was tagged by Facebook and shipped to police, who arrested the man.

The FBI says it's on board with this technology and hopes more online sites use it.

**What do you think? Should you have privacy when it comes to personal chats? Click the link and let us know.**

NEWS & FEATURES | Jul 20th, 2012

# Your Facebook Chats are Being Monitored, Find Out Why: The Social Media Privacy Report

Jillian Ryan

What you say in your private chats and messages on Facebook may not be as private as you think. According to a recent report from Reuters, the social media giant employs a mums-the-word technology that scans posts and chats for criminal activity. If something is fishy, the content is flagged and then read by an employee who will access the conversation and call the police, if necessary.

This monitoring came to light, when, earlier this year, a man is his thirties was Facebook chatting with a 13-year old female minor from South Florida. The two were talking about sex and planning to meet after school. However, with Facebook's assessment, the police were able to commandeer the teenage girl's computer. According to Special Agent Supervisor Jeffrey Duncan of the Florida Department of Law Enforcement, the fast pace flow of information provided by Facebook allowed for the arrest of the suspect in question.

Reuters reports that Facebook's "efforts generally start with automated screening for inappropriate language and exchanges of personal information, and extend to using the records of convicted pedophiles' online chats to teach the software what to seek out." The system also analyzes patterns of behavior. As a filter, it seeks out users who exchange abusive language and contact information. However, it also goes a step further to examine "whether a user has asked for contact information from dozens of people or tried to develop multiple deeper and potentially sexual relationship, a process known as grooming."

Facebook's Chief Security Officer, Joe Sullivan, is very clear when he notes that, "We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate," he said. Additionally, he noted that Facebook doesn't focus on pre-existing friendships.

While Facebook is taking some measure to ensure user privacy, some may say that even though thwarted sexual predators is a moral good, the invasion of personal information crosses the line. According to the Help Center's Law Enforcement and Third-Party Matters on Facebook, the site states, "We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law…We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities."

Do you think that Facebook is doing social good by monitoring user conversations? Or do you believe that such surveillance of private dialogues is a blatant invasion of privacy? Weigh in below by leaving a comment.

the INQUIRER

Search

*Fiction reveals truth that reality obscures - Jessamyn West*

Home | News | Reviews | Video | INQdepth | Downloads store | Debates | App

Communications > Security

# Facebook scans private chats and posts for criminal activity

Contacts authorities when a conversation has been flagged as unlawful

By **Lee Bell**

Fri Jul 13 2012, 16:25

**SOCIAL NETWORK** Facebook scans private chats and posts for criminal activity, it has been revealed.

A Reuters interview with a special agent supervisor for the Florida Department of Law Enforcement, Jeffrey Duncan revealed that the social network contacts the authorities when a conversation has been flagged as potentially criminal activity.

"A man in his early 30s was chatting about sex with a 13-year-old South Florida girl and planned to meet her after middle-school classes the next day, the article reads.

"Facebook's extensive but little-discussed technology for scanning postings and chats for criminal activity automatically flagged the conversation for employees, who read it and quickly called police. Officers took control of the teenager's computer and arrested the man the next day."

In the interview, Duncan praises Facebook for triggering inquiries,

"The manner and speed with which they contacted us gave us the ability to respond as soon as possible," he said.

Facebook's security tool focuses on conversations between users who aren't friends or recently became friends on the network and have few or no mutual friends.

The tool also places enphasis on members who have a significant difference in age and are located far from one another to gain a better chance at finding offenders.

Facebook is yet to respond to our request for comment, but in the Reuters article Facebook's chief security officer Joe Sullivan said, "We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate."

This adds yet another security concern for social network users. Privacy is a sensitive subject for Facebook, which has been criticised many times already for its sloppy and ineffective attempts to protect its users from violations of their privacy.

Sophos' senior security consultant Graham Cluley said, "It shouldn't surprise anybody that Facebook is trying to make its site a safer place by monitoring for illegal and suspicious behaviour which might bring it into disrepute.

"Obviously we have to hope that Facebook acts responsibly, and puts measures in place to prevent inappropriate monitoring - or risk a backlash from users." µ

Comment on this article | Flame Author | Print

Tags: **Security**

**Share this:**

Most read | Most commented | Most watched

- Apple Watch price, release date and specs
- Galaxy S6 pre-order, release date, specs and price
- Taxpayers will spend £1m buying MPs iPad tablets
- Apple buys and closes database firm FoundationDB
- NI schools flushed with free Minecraft in next-gen coder drive

**INQ Poll**

**Amazon Twitch hack**

Do you make sure your passwords are secure?

○ Yes, I use auto password generators

○ Yes, I always use a mix of symbols, letters and numbers

○ Yes, I use biometrics

○ I use the same password for everything

○ As above - and it's written on a Post-it note

● I use passw0rd and my PIN number is 0000

» View other polls

Vote

del.icio.us Digg Facebook Linkedin Linkedin reddit!
StumbleUpon Twitter Share

## Related articles

Kim Dotcom is bankrupt and possibly doomed

Apple will pay you to ditch your Android or BlackBerry...

Reborn Pirate Bay could be an FBI honeypot

Amazon warns of Twitch data breach

Recommended by Outbrain

< Previous article | Next article >

blog comments powered by Disqus

Home | News | Reviews | Video | INQdepth | Downloads store | Debates | App

incisivemedia

Search

| | |
|---|---|
| **Site Credentials:** | About us \| Terms & Conditions \| Self Service Advertising \| Privacy policy \| About Incisive Media \| Sitemap |
| **Follow us:** | Youtube \| Twitter \| Facebook \| Linkedin \| |
| **Business & Technology websites:** | V3.co.uk \| CRN UK \| Computing \| Business Green \| Cloud Hub \| Search Engine Watch \| ClickZ \| |
| **Business research resources:** | B2B Web Seminars \| Business Technology Video \| Whitepapers \| |
| **Products:** | Software Reviews \| Hardware Reviews \| Download Reviews \| |
| **Accreditations:** | aop 2010 WINNER aop 2013 WINNER Digital Publisher of the Year 2010 & 2013 \| |

WebProNews

ADVERTISE TIP US FOLLOW SEARCH

Home Search Social eCommerce Advertising Business Tech Developer All

# Should Facebook Monitor Chats to Help Snag Child Predators?

By Josh Wolford August 23, 2012 · 0 Comments

SUBSCRIBE FREE 400K+

- Stur Like 106 g+1 8 Tweet Flip

[ Social Media ] Let's face it; social media and privacy are always going to be two warring parties. Sure, privacy controls help users define *who* can see *what* on sites like Facebook, Twitter, and Pinterest (and some sites offer simpler, more accessible privacy options than others). But in the end, social networks are social – you're actively sharing content with the world. Anybody who thinks they can maintain a pristine level of privacy and security while still enjoying the benefits of a social community is probably deluding themselves.

Facebook is no stranger to user privacy scandals. Scenarios involving information sharing and user tracking have popped up in the last couple of years. The FTC has even stepped in and performed their own investigations.

And recently, it was revealed that Facebook actively patrols user communications for unlawful activities. **Is this a privacy betrayal from a company that sits on so much personal information about the country's inhabitants? Or is it a social good that allows Facebook to help prevent violent crimes, especially those involving children?** Let us know in the comments.

A Winnipeg man is being charged with sexual assault, sexual interference, and internet luring after Facebook intercepted communications between him and a 13-year-old girl. According to Winnipeg police, the chat messages were sexual in nature, and were brought to their attention by Facebook near the end of July.

If the phrase "Facebook intercepted communications" caught your attention, I don't blame you. And I can't say that it's not exactly what you're thinking – Facebook is actively monitoring our chats and messages. Early last month, the company revealed that it's common practice for their teams to scan chats, searching for criminal activity. It's mostly algorithms that handle this part, but once something is flagged Facebook employees make the final decision on whether or not it merits calling the authorities.

Facebook algorithms give more weight to communications between users that don't really have a lot of connections. If two users have a giant age difference or live all the way across the country from each other – the conversation may be flagged. If two users don't share many friends or have never interacted with each other before on the site – their conversation may be flagged.

So it's fair to say that the "bad apple" conversations are going to be the ones most frequently caught up in the machine. But the final screening process for reporting malicious activity means that human eyes have to look at the chat transcripts – at least every now and then.

**Vine Videos Will Soon Be Much Prettier**
Quality enhancements
0 Comments

**Here's How To Use Twitter's New Periscope App**
What to do with it and what not to do with it
0 Comments

**Should You Use Facebook Comments On Your Site?**
Facebook revamps comments plugin with helpful new feature
1 Comment

**Super Troopers 2 Hits Crowdfunding Goal in a Day**
Mother of God
1 Comment

**Facebook Finally Lets You Embed Facebook Videos**
Yay!
1 Comment

**360-Degree Videos: Coming Soon to Facebook News Feed**
f8
1 Comment

**Facebook Launches Blueprint To Teach You Some Things**
It's kind of like a Khan Academy for Facebook marketing
0 Comments

**Facebook Wants to Keep Those Videos Coming**
Forever and ever and ever and ever

Back to Winnipeg, and to the 25-year-old man who was sending sexual messages to the underage girl. Authorities say that Facebook described the chats to them as "inappropriate" and "explicit."

Although Facebook notified police of the chats in late July, the suspect wasn't arrested until early last week.

And according to CNEWS, a sexual assault had already taken place. There's no word on whether the police received the tip from Facebook before or after the alleged assault.

So, police now have the Facebook data to use in prosecution, but it didn't actually stop a young girl from being sexually assaulted. It's unclear if that's because Facebook caught it late, police failed to act in time, or the assault had already occurred before anyone caught wind of the inappropriate chats. Really, it's not right to blame anyone here except the pedophile who allegedly performed the violent acts – but it does show that Facebook's monitoring program isn't perfect.

However, it also demonstrates that it's possible for Facebook to do some good with their chat monitoring. It's also worked before (to perfection), according to Facebook.

When the chat monitoring story first broke, Facebook told Reuters a story of how the program had led to the arrest of a man who was in the process of soliciting a 13-year-old girl on the network. Here's how Reuters told it:

> *A man in his early thirties was chatting about sex with a 13-year-old South Florida girl and planned to meet her after middle-school classes the next day. Facebook's extensive but little-discussed technology for scanning postings and chats for criminal activity automatically flagged the conversation for employees, who read it and quickly called police.*
>
> *Officers took control of the teenager's computer and arrested the man the next day, said Special Agent Supervisor Jeffrey Duncan of the Florida Department of Law Enforcement. The alleged predator has pleaded not guilty to multiple charges of soliciting a minor.*
>
> *"The manner and speed with which they contacted us gave us the ability to respond as soon as possible," said Duncan, one of a half-dozen law enforcement officials interviewed who praised Facebook for triggering inquiries.*

There's really no denying than it can work. Scanning chats for suspicious activity can help to thwart child predation.

Of course, there are still privacy concerns to consider. Not everyone is convinced that Facebook has the right to monitor "private" communications. Then again, you are using their (free) service to send and receive communications, and at least now it's with the public knowledge that the company may be monitoring them. Plus, they are not the only ones engaging in this type of monitoring.

Facebook won't comment on the particulars of the Winnipeg case, but they tell me that they have zero tolerance for this type of activity and are "extremely agressive" in reporting it to the authorities.

Here's their full statement:

*We have zero tolerance for this activity on Facebook and are extremely aggressive in preventing and identifying inappropriate contact as well as reporting it and the people responsible for it to law enforcement. We're constantly refining and improving our systems and processes. However, we feel we've created a much safer environment on Facebook than exists off-line, where people can share this material in the privacy of their own homes without anyone watching.*

**Have they created a "much safer environment?" In your opinion, is it okay for Facebook to patrol chats in order to help identify possible criminals? Is it a good program conducted in good faith? Is it worth giving up a little bit of your privacy for the greater**

2 Comments

**Facebook Walks You Down Memory Lane**

Tries Not to Throw You in Terrible Memory Ditch

3 Comments

**Would You Let Facebook Host Your Content?**

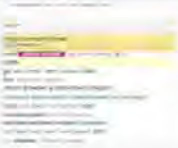
It's partnering with some publishers to do just that

2 Comments

**Add Value To Your Content With Reddit Embeds**

Reddit launches embeddable comment threads

0 Comments



**Twitter Takes First Proactive Step to Fight Abuse**

New feature called quality filter

2 Comments

**Instagram Finally Launches Its Own Photo Collage App**

Layout

1 Comments

**Why Aren't Brands Taking Advantage Of Instagram?**

Yesmail offers some thoughts

0 Comments

**Shockingly Low Percentage Of Brands On Instagram**

Report suggests brands are

**good?**

**Or do you think that Facebook should cease this type of monitoring?** Let us know in the comments.

0 Comments

Share on Facebook

RELATED ITEMS CRIME FACEBOOK MESSAGES ONLINE SAFETY PRIVACY

**About Josh Wolford**
Josh Wolford is a writer for WebProNews. He likes beer, Japanese food, and movies that make him feel weird afterward. Mostly beer. Follow him on Twitter: @joshgwolf Instagram: @joshgwolf Google+: Joshua Wolford StumbleUpon: joshgwolf
View all posts by Josh Wolford →

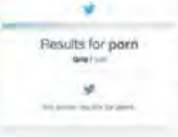
**Top Rated White Papers and Resources**

missing out big time

0 Comments

**Twitter: We're Not Blocking Porn on Purpose**
Just a bug

0 Comments



**Facebook Messenger Will Now Let You Send Money**
For free

0 Comments

**Twitter Makes Reporting Threats to Police Easier**
One more step to a safer service

0 Comments

NEXT ARTICLE »

Advertise | About Us | Newsletter | News Feeds | Terms & Conditions | Contact Us

**WebProNews**
WebProNews is your comprehensive resource for news, information, and tips related to online business

**DevWebPro**
DevWebPro is dedicated to bringing you the best developer information on the net.

**GetIP**
A free application that helps users find out the details of their internet connection, as well as that of any other IP address or domain.

**PRtracking**
A free automated PageRank checking service

**Twellow**
Twellow is a directory of public Twitter accounts, with hundreds of categories and search features to help you find people who matter to you.

**Company**
Corporate
Advertising
Sitemap
Newsletters
Privacy Policy
About Us
Contact Us

**iEntry Network**
Web Developers
IT Managers
Small Business Owners
eBusiness Management
Software
Gamers

**Advertising**
Why Advertise?
Who's Advertising?
Testimonials
Newsletter Samples
Ad Space
Contact

**Get to know us**
iEntry Network, a business-to-business Web media services company, provides your pathway to over 8 million IT professionals, small business owners and ecommerce entrepreneurs, marketing professionals, industry bloggers, and Web-savvy media consumers.

# Facebook Knows When You're Chatting About Your Illegal Activities

Kate Tummarello - *Staff Writer, InTheCapital*
*07/13/12 @8:05am in* Business

335

If you're committing or planning to commit a crime, it's probably not best to talk about it on Facebook. While you may think that you're safe as long as you don't publicly post about it on anyone's wall or upload pictures (how are there people who this??), but it turns out that even confining your talk of illegal activity to private Facebook chats.

According to online reports, Facebook uses a software that screens private chats to determine if participants are discussing illegal activities.

A Mashable article from earlier this week on the topic explains how the software determines which conversations might include useful information about illegal activities:

> The screening process begins with scanning software that monitors chats for words or phrases that signal something might be amiss, such as an exchange of personal information or vulgar language.
> The software pays more attention to chats between users who don't already have a well-established connection on the site and whose profile data indicate something may be wrong, such as a wide age gap.
> The scanning program is also "smart" — it's taught to keep an eye out for certain phrases found in the previously obtained chat records from criminals including sexual predators.
> If the scanning software flags a suspicious chat exchange, it notifies Facebook security employees, who can then determine if police should be notified.

Facebook repeated to Mashable a statement originally issued to Reuters,who first reported on the social network's chat tracking tools. "We've never wanted to set up an environment where we have employees looking at private communications, so it's really important that we use technology that has a very low false-positive rate," the company said. By keeping most of the private chat records away from employees, Facebook is protecting itself from some privacy advocates, the Mashable article explains.

[Image via Facebook]