# 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


Would you want

**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.**

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

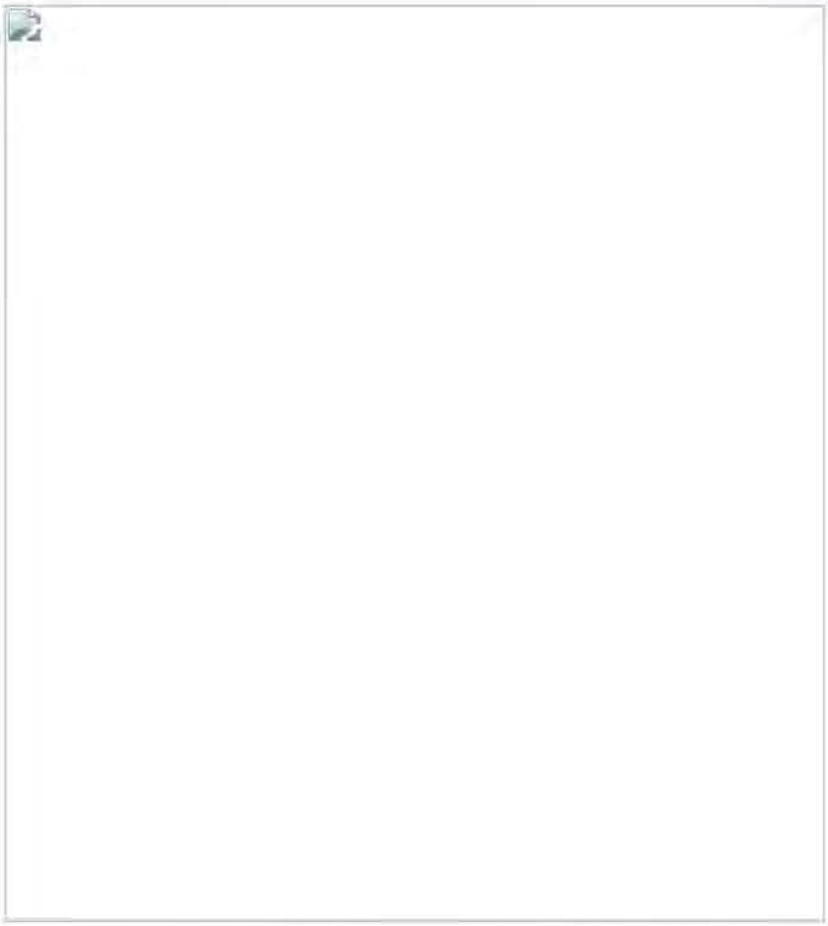
Facebook
Internet
Child protection
Children
Social networking

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.

# 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.

# 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



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

## 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



< Previous article | Next article >