EXHIBIT J

total number of likes, which is actually by design. Some users find the sincerity of such a practice nebulous at best, however.

Confirming the discovery, Facebook said, "*We did recently find a bug with our social plug-ins where at times the count for the Share or Like goes up by two, and we are working on fix to solve the issue now.*"

Facebook reiterated though that some behaviors will generate likes without explicitly liking something, such as messaging a URL to a friend. On Facebook for Developers, the BBC points out though, there are actually four ways to generate likes. However, only one of those methods actually requires users to click a like button. The rest are done behind the scenes.

Last month, the social networking icon kick started an intitiative which intends to fortify the integrity of Facebook's likes and shares. Amongst the improvements, automated tools were deployed with the intent of deleting disingenuous likes that were determined to be purchased or originate from malware or compromised accounts

Links shared privately on Facebook increase page's Like count

by KS Sandhya Iyer, 5 October 2012

Back in August Facebook had announced that it had 955 million active monthly users as of June 30, up 29 percent from a year earlier. Bit it also estimated that as many as 8.7 percent of those accounts, or a tad over 83 million, are fake.

More recently, there were reports of Facebook making 'efforts' to weed out fake profiles that are being created by computer programs, which are used for inflating the number of "likes" on a Facebook page for a brand.

In that respect, The Next Web makes an interesting observation. The tech blog reports that when a Facebook user sends a link to a Web page through a private Facebook message, that Web page will get not one but two extra "Likes," if it is a Facebook-"Like"-able Web page.

The site stumbled upon a YouTube video (now deleted) on Hacker News posted by Polish start-up Killswitch.me that clearly showed how sending a private Facebook message containing a link to a page increased the counter on that page by two "Likes".

Considering whether or not the two Likes was a bug, Facebook issued a statement saying:

> *"We did recently find a bug with our social plugins where at times the count for the share or like goes up by two, and we are working on fix to solve the issue now. To be clear, this only affects social plugins off of Facebook and is not related to Facebook page likes. This bug does not impact the user experience with messages or what appears on their timelines."*

The blog thus simplified it to state that Facebook is keeping an eye on your private

IN THE STORES

POPULAR RIGHT NOW

How to Activate WhatsApp Calling


Facebook is Down for Several Users Around the World


Samsung Galaxy S6, Galaxy S6 Edge to Be Manufactured for India at Noida Plant


How to Make a Bootable USB Disk for Windows 8, Windows 7, Windows XP


WhatsApp Voice Calling - Everything You Need to Know


iPhone 6S, iPhone 6S Plus, iPhone 6C to Launch This Year: Report

FORUM »

Smartphones under or upto 16000
5 Replies,
Latest Post by

Is lenovo a6000 worth buying...?
27 Replies,
Latest Post by

Please suggest me a smartphone under 25k
5 Replies,
Latest Post by

Help me in selection of Mobile (Android)
8 Replies,
Latest Post by

messages for URLs that have Like buttons and should be increased. The Next Web further pointed out that the Like button entry on the Facebook Developers page states that the number shown on Like buttons on other websites is a total of likes of that URL, shares of that URL, likes and comments on Facebook stories about that URL and inbox messages containing that URL as an attachment.

So the question is, how big a deal is it and does it invade Facebook user privacy? Probably not - and here's why. That "Like" is only added to the page's counter. It does not reveal who added the Like. If you do not reveal something said or shared in private to others, you are not invading their privacy. Here's how Facebook clarified on the issue:

> *Absolutely no private information has been exposed and Facebook is not automatically Liking any Facebook Pages on a user's behalf. Many websites that use Facebook's Like, Recommend, or Share buttons also carry a counter next to them. This counter reflects the number of times people have clicked those buttons and also the number of times people have shared that page's link on Facebook. When the count is increased via shares over private messages, no user information is exchanged, and privacy settings of content are unaffected. Links shared through messages do not affect the Like count on Facebook Pages.*

Facebook isn't going to be axed for this move for the simple reason that email providers like Gmail scan user emails all the time. It does so to show relevant ads, fight spam, and slow down viruses. What Facebook is doing is just adopting one of the many services of tracking the popularity of Webpages. While Google has a list of trends. The New York Times keeps a track of most emailed stories.

Facebook issued an updated statement to The Next Web giving further clarification:

> *Our systems parse the URL being shared in order to render the appropriate preview, and to also ensure that the message is not spam.*

What Facebook is likely more concerned about is why the Like count is increased by two instead of one, and said it will investigate the bug.

Tags: Facebook, Facebook Like button, Facebook page Like, Facebook private message

Share

< *YouTube alienates amateur users by courting pros*

Microsoft to release updates for built-in Windows 8 apps >

COMMENTS

Sign in using or

Phones below 15K
31 Replies,
Latest Post by

JOIN THE DISCUSSION

DON'T MISS

SOCIAL NETWORKING»

Facebook is Down for Several Users Around the World

Meerkat Raises $14 Million in Funding as Twitter Launches Periscope

Twitter Launches Periscope Live Video Streaming App to Rival Meerkat

Drones Beaming Web Access Are in the Stars for Facebook

Ten Big Announcements From Facebook's F8 Developer Conference

More Social Networking »

IN MOBILES AND TABLETS »

Latest	Popular
ZTE Nubia Z9 Mini	Xiaomi Mi 4
ZTE Nubia Z9 Max	Samsung Z1
Celkon Millennia Q450	Lenovo A6000
Rio New York	Micromax Yu Yureka
Rio Paris	Xiaomi Redmi Note 4G
Rio London	Google Nexus 6
Lava Iris 414	Xiaomi Redmi 1S
Zebronics Zebpad 7T500	Lava Iris Fuel 50
Lenovo K3 Note	Motorola Moto G (Gen 2)
iBall Slide Q40i	Asus ZenFone 5
Intex Aqua Xtreme V	Motorola Moto E
Meizu m1 note	Xiaomi Mi 3
Sony Xperia J1 Compact	Micromax Unite 2
	Asus ZenFone 4

Post to Facebook Post to Twitter Login & Comment

Hot Topics:

Harry Reid
Germanwings Crash
Bowe Bergdahl
Ted Cruz
Israel
TheBlaze TV

Technology

Why Is Privacy of Personal Facebook Messages Being Called Into Question – Again?

Oct. 5, 2012 12:30pm Liz Klimas

(Image: Shutterstock.com)

A rumor that Facebook was revealing your private messages on Timeline was recently raised and debunked, but a new concern regarding private conversations and the potential for "'like' fraud" has come to light.

The Wall Street Journal reports that Hacker News has revealed a method that "let's you pump up to 1800 'Likes' in an hour." How is this done? Hacker News posted a video showing the exploit, revealing that including links in private messages — if these links had a "like" button associated with them –would increase the "likes" on that actual page by two.

(Editor's Note: The YouTube video was taken down for "depiction of harmful activities." The group posted a version of it on Vimeo as well, but TheBlaze is not embedding the video to show how the hack works because it includes graphic, NSFW photos.)

The Next Web's Emil Protalinski explains the implications of this exploit as such: "Facebook is monitoring your private messages for links that have Like buttons and should be increased."

The Hacker News users' video states that they see this as leading to "'like' fraud."

Facebook has responded saying that there was a bug identified in the system that was accidentally counting one "like" or "share" of a link or post as two. It states it is working to fix this. But in a statement reported by WSJ and others, Facebook emphasized that "no private information has been exposed." Meaning, if you receive a message containing a link that has a "like" button, you are not automatically "liking" this item on your Timeline.

"Many websites that use Facebook's 'Like', 'Recommend', or 'Share' buttons also carry a counter next to them. This counter reflects the number of times people have clicked those buttons and also the number of times people have shared that page's link on Facebook," including over private messages," Facebook said in a statement.

Still, Paul Shea for Value Walk writes it's probably news for many that the "like" counter is not just measuring clicks but sharing content as well — in the form of private messages in this case. Protalinsky for TheNextWeb outlines the specifics for how this works:

> *[...] on the Like button Web page over on Facebook Developers, the social networking giant says the number shown on a Like button is the sum of:*
>
> The number of likes of this URL.
> The number of shares of this URL (this includes copy/pasting a link back to Facebook).
> The number of likes and comments on stories on Facebook about this URL.
> The number of inbox messages containing this URL as an attachment.

Shea writes that Facebook has "not crossed a line with this latest news, any more than they have on hundreds of other occasions." Shea says he only expects the company will continue to experience backlash over privacy concerns "for as long as it operates."

Related:

Would You Pay for More People to See Your Facebook Posts? Now You Can
'Credibility Is Dissipating': Do You Trust Google or Facebook?
Are Facebook's Design Improvements Tricking You Into Giving Up Privacy?
Facebook's Proposed Privacy Policy Updates Expand 'Data Collecting Tactics'

Featured image via Shutterstock.com.

Related:

Cyber Security,
Facebook

POPULAR STORIES ON THE BLAZE

'Duck Dynasty' Star Phil Robertson Under Fire Over Graphic Comments About Atheists, Rape and Murder 885 Comments

Watch How Ted Cruz Responds When He's Asked on CBS If He Would 'Take' Away Health Care From 16 Million People as President 510 Comments

Pastor Says Christians Have So Terribly Handled This Issue That It Will Be the 'Talk of the Church for the Next 10 to 15 Years' 392 Comments

The Message Glenn Beck Got in the Middle of His Special on Grover Norquist That Will Affect the Rest of the Week 336 Comments

MSNBC Realized in Minutes They Had to Apologize for Guest's Jaw-Dropping Attack on Ted Cruz, Country Music 298 Comments

SIGN UP FOR OUR DAILY EMAIL NEWSLETTER!

Enter your email address Sign Up

Embed TheBlaze Headlines on Your Own Site!

Faith

Actor Expresses 'Outrage' and Calls for a Boycott Over Indiana's 'Religious Freedom' Law Read More

The Abortion Statistics Surrounding American Millennials That Might Surprise You Read More

The New Country Music Song That Has Some Fans Outraged and Calling for Boycotts — but Does It Really Promote the 'Gay Agenda'? 129 Comments

Politician's Shocking Explanation for a Woman's Baby Being Cut From Her Womb Involves a 'Prophetic' Message and the Bible Read More

Pat Robertson's Claims About Liberals, Radical Islam and 'Decapitating People' Stir Controversy 154 Comments

Business

Watch Disneyland Get Built From the Ground Up in Just One Minute Read More

Reporter First Thought the Comment He Received From Google Was a Joke. It Wasn't. Read More

RadioShack Auctions Off Millions of Customers' Names and Information, Despite Its Privacy Policy Read More

These Five Industries Hold All the Cards When It Comes to American Jobs Read More

A Mega-Merger Just Created a Food 'Powerhouse' Read More

Technology

Watch This 'Star Wars' Drone Shoot 'Lasers' Across the Sky Read More

After Their Cars Broke Down, 10 Drivers Discovered They Had One Thing in Common: Visiting This Gas Station Read More

National Investigation Reveals Alarming Number of Attacks on U.S. Power Grid Read More

No, Ted Cruz Is Not a Nigerian Prince Scammer Read More

Ford's Latest Technology Involves Using Cameras to Keep You From Driving Too Fast, but Is That Really All They Will Do? Read More

The Blog

Obama says the rich 'really don't need a tax cut'

This may be one of the most awkward Obama Introductions ever — watch what happens

The administration's surprising claim about how it will fund Obama's immigration plan

'Grover Norquist: The Glenn Beck Interview' live chat and fact check

Disgraced Rep. Aaron Schock looks to Abraham Lincoln for inspiration as he starts his 'new chapter' in life

The Wire

$2,000 offered in case of woman found shot near Johnstown
Swedish poet Tomas Transtromer dies at 83
Swedish publisher says poet and Nobel Prize winner Tomas Transtromer has died at age 83.
Fitch Places Cathedral Village (PA) on Rating Watch Positive
Former Alabama police officer indicted on federal charge in confrontation with Indian man
Asbestos Disease Awareness Organization (ADAO) Praises Senate for Passing the Bipartisan 11th Annual "National Asbestos Awareness Week" Resolution
Ex-child welfare agency head guilty of stealing $68,000
The Latest: Europe aviation agency urges 2 crew in cockpits

Facebook private messages trigger 'likes' without telling

Ed Oswald (/author/Ed-Oswald/) | @edoswald
PCWorld Oct 5, 2012 7:34 AM

The next time you share a link with a Facebook friend via private message, be aware that you're anonymously "liking" that page publicly as well.

That's what developers with Polish startup Killswitch.me (http://signup.killswitch.me/) discovered while researching other issues surrounding the "like" button. They stumbled upon the fact that sending a message to a friend with a likable link triggers an anonymous like of that page.

While this may come as a surprise, evidence that the company was scanning our messages for these likable links has been public for at least a week. Facebook states in a September 27 FAQ for developers (https://developers.facebook.com/docs/reference/plugins/like/) that "the number of inbox messages containing this URL as an attachment" is a factor in counting the number of likes that shows up on a page's Like Button.

Other factors include the number of actual likes, the number of shares (including a share on Facebook), and the number of likes and comments on stories on Facebook about the URL.

While this information seems to have been public for some time, those of us who aren't developers likely had no clue of Facebook's actions. That said, given how Facebook uses our activities to further its own business interests, this practice shouldn't surprise us. Facebook routinely relies on its members' personal information when it comes to serving more targeted ads (http://www.pcworld.com/article/230757/help_a_web_ad_is_stalking_me.html?tk=rel_news).

Personal messages seem to be another matter, however. We may privately share something with a friend that we'd rather not make public. Facebook seems to acknowledge that, assuring The Next Web

(http://thenextweb.com/facebook/2012/10/04/facebook-confirms-it-is-scanning-your-private-messages-for-links-so-it-can-increase-like-counters/) that the mention of the link merely adds an anonymous "like" and that no page or link is automatically liked on the user's behalf, nor does it appear on a user's timeline.

Will this appease privacy critics and uneasy users? As long as this remains Facebook's policy, it should. But Facebook should be warned: a recent study (http://aisel.aisnet.org/amcis2012/proceedings/SocialIssues/3/) by researchers at New Jersey Institute of Technology and Pace University shows that users are paying attention, and will respond if they feel their privacy is threatened.

Compared with Facebook users five years ago, today's Facebookers are much more engaged in protecting their privacy, and more "proactive" when it comes to responding to incidents that may affect their privacy on the site, researchers say.

Related: Social Networks (/Tag/SocialNetworks/)

Facebook (/Tag/Facebook/)

Ed Oswald

Ed is a technology journalist, music nut, and gadget geek who hails from the somewhat small town of Reading, Pennsylvania.

More by Ed Oswald (/author/Ed-Oswald/)

COMMENTS

nakedsecurity
Award-winning computer security news from SOPHOS

Facebook scans private messages to inflate the "Like" counter on websites

by Lisa Vaas on October 8, 2012 | 8 Comments
FILED UNDER Facebook, Privacy, Social networks

Facebook has confirmed that it's scanning private Facebook messages to boost "Like" counters on third party websites.

Killswitch.me, described by The Next Web as a "Polish startup", on Thursday posted a since-deleted YouTube video on Hacker News that showed that sending a link to a website via a private Facebook message increased that website's Facebook Like counter by two likes.

And then by another two. And then another, and another, causing the Likes to steadily balloon.

In fact, one poster on Hacker News testified that people could pump it up by 1,800 Likes per hour.

The video, removed from YouTube, can still be viewed on Vimeo (possibly not safe for work).

When TNW's Emil Protalinski checked with Facebook, company spokespeople confirmed that they had discovered a bug affecting Like counts.

But the bug didn't relate to the actual private-message peeping.

Rather, the bug concerned inflating page counts by two Likes instead of one, as a spokesperson told TNW:

> We did recently find a bug with our social plugins where at times the count for the Share or Like goes up by two, and we are working on [a] fix to solve the issue now. To be clear, this only affects social plugins off of Facebook and is not related to Facebook Page likes. This bug does not impact the user experience with messages or what appears on their timelines.

The fact that this is function is baked into Facebook code as opposed to being a potential fluke of privacy transgression is confirmed, as Protalinski noted, on the Facebook Developers page, which states that a websites' number of Likes is the sum of:

> * The number of likes of this URL
>
> * The number of shares of this URL (this includes copy/pasting a link back to Facebook)
>
> * The number of likes and comments on stories on Facebook about this URL
>
> *The number of inbox messages containing this URL as an attachment.

Facebook's scanning of private messages isn't new.

The power of the social media mammoth's data mining technology when applied to private messages came to light in March, when Facebook was credited with quashing potential child molestation between a 13-year-old girl and a man in his 30s who were having a private Facebook conversation about sex.

As Facebook described it at the time, its data mining technology scans postings and chats for criminal activity, analyzing relationships to find suspicious conversations between unlikely pairings: i.e., between people of widely varying ages who only have loose and/or newly formed relationships.

Email providers such as Gmail also have a long-standing practice of reviewing messages to weed out spam and to target ads.

Those are reasonable uses of data mining technology, but it's disconcerting to find what might be yet more intrusive forays into allegedly private messages.

Thus, it's a bit of a relief to learn that Facebook later clarified the privacy issue, saying that "absolutely no private information" is exposed in the private-message-derived Like inflation:

> Absolutely no private information has been exposed and Facebook is not automatically Liking any Facebook Pages on a user's behalf.
>
> Many websites that use Facebook's 'Like', 'Recommend', or 'Share' buttons also carry a counter next to them. This counter reflects the number of times people have clicked those buttons and also the number of times people have shared that page's link on Facebook. When the count is increased via shares over private messages, no user information is exchanged, and privacy settings of content are unaffected. Links shared through messages do not affect the Like count on Facebook Pages.

At any rate, the integrity of the Facebook Like counter has been in question for a while.

It came up again last week, when well-Liked pages began to sag as Facebook swept out bogus Likes gained via malware, compromised accounts, duped users or purchased bulk Likes.

Unfortunately,the fact that Facebook registers URLs shared in private messages means that we're now all potentially contributors of unintended likes.

It means that sharing a link that outrages, disgusts or appalls the sender will result in that website's Facebook Like counter going up.

Researching hate groups? Discussing corporate malfeasance?

Be prepared to add to your subjects' Facebook counter glow, whether you want to or not, if you send URLs via private Facebook conversations.

If you're on Facebook, and want to learn more about security and privacy issues on the social network, consider joining the **Naked Security Facebook page**.

Private stamp, courtesy of Shutterstock

Tags: data mining, Facebook, page Likes, private messages, scanning

You might like

Facebook wages war on Like-baiting and spammy posts

Facebook is being sued for intercepting users' communications

Selena Gomez's Facebook account hacker jailed for one year

Embarrassing privacy flaw found on Facebook

8 Responses to *Facebook scans private messages to inflate the "Like" counter on websites*

Cathy Moore Pritchett · 900 days ago

I would like to share this on Facebook to warn my friends but there's no Facebook share button. How do I share?

0 0 Rate This

Reply

Dawn Jasmann · 899 days ago

Cathy, you can share ANY website on Facebook just by highlighting the address in the address bar, copying it, then pasting it in the status update box on your Facebook page. It's that simple. :)

P.S. I usually comment about what I'm about to share BEFORE pasting the website address into my status update box. That way my comment gets seen on top of the address. For example:

Check out this website. I think you'll find it as interesting as I did. https://nakedsecurity.sophos.com/2012/10/08/facebo...

0 0 Rate This

Reply

Richard · 899 days ago

If you "Like" Naked Security on Facebook, they post links to these articles on there, and then you can easily share them.

0 0 Rate This

Reply

Doc · 899 days ago

Copy & Paste the Link to FB.

0 0 Rate This

Reply

aLikeable Guy · 899 days ago

So, if you send a link along with a comment "This is the stupidest thing I have ever seen." It gets 'Liked" ?

Awesome.

1 0 Rate This

Reply

Yitzchok Mickler · 898 days ago

I have a Facebook sharing button on this page. Look at the end of the article just before "How likely are you to recommend Naked Security to a friend or colleague?"

0 0 Rate This

Reply

davepeterson1 · 898 days ago

I've lost count of the times failbook does evil sleazy things like this, it's so INFURIATING.

0 0 Rate This

Reply

nikhil · 896 days ago

nikhil · 890 days ago

no .. its not like what you are thinking, its because of java-script used by the website on that page. I have tested it on 4 website, but website having same java-script code of Facebook likes gets incremented while which does not , it remain same as it is. So there is no risks of reveal of private messages,

0 0 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

FB000000346

MarTech

CMO

Social

Search

Consumer

Your Private Facebook Messages Aren't So Private: Shared Links Count Towards 'Like' Data

Greg Finn on October 8, 2012 at 9:33 am

See that "Like" button just above this sentence? The majority of folks think that the number displayed is made up of all those who've actually "liked" this article. It's not the case however — the Like button is an aggregate score from a variety of Facebook actions, including links shared within private messages.

TheNextWeb uncovered a bug last week that was actually providing two Likes for data shared privately. Facebook did confirm that the issue of double counts was a bug, but did also confirm that shared messages do count towards the overall "like" data. In fact the Facebook Developers page clearly states the following about Like buttons:

> The number shown is the sum of:
>
> - The number of likes of this URL
> - The number of shares of this URL (this includes copy/pasting a link back to Facebook)
> - The number of likes and comments on stories on Facebook about this URL
> - The number of inbox messages containing this URL as an attachment.

The fact that private shares gave an endorsement (even if an anonymous one) drew a bit of an uproar. What if users were sharing a link of a product that they didn't like? Well, it will still be counted as a "like." In fact every time that a link is privately it counts as an additional Like on the Like button. Facebook gave TheNextWeb the following statement on the private message "likes:"

> Absolutely no private information has been exposed and Facebook is not automatically Liking any Facebook Pages on a user's behalf.
>
> Many websites that use Facebook's 'Like', 'Recommend', or 'Share' buttons also carry a counter next to them. This counter reflects the number of times people have clicked those buttons and also the number of times people have shared that page's link on Facebook. When the count is

> increased via shares over private messages, no user information is exchanged, and privacy settings of content are unaffected. Links shared through messages do not affect the Like count on Facebook Pages.

We've reached out to Facebook for more data on the Like button. For more information see TheNextWeb.

ABOUT THE AUTHOR

Greg Finn

Follow @gregfinn

Greg Finn is the Director of Marketing for Cypress North, a company that provides world-class social media and search marketing services and web & application development. He has been in the Internet marketing industry for 10+ years and specializes in Digital Marketing. You can also find Greg on Twitter (@gregfinn) or LinkedIn.

RELATED ARTICLES

Get Real: Facebook Asking Users To Rat Out Friends Who Aren't Using Real Names

FTC Approves Facebook Privacy Settlement Reached Last November

Senate Hearing To Examine Facebook's Facial Recognition

Norway Investigating Facebook Facial Recognition Tagging

CHANNEL: CONSUMER | FACEBOOK | FACEBOOK: PRIVACY | FEATURES & ANALYSIS | TOP NEWS

(Some images used under license from Shutterstock.com.)

LEARN MORE ABOUT OUR SMX EVENTS

MARTECH
THE MARKETING TECH CONFERENCE

MarTech: The Marketing Tech Conference is for marketers responsible for selecting marketing technologies and developing marketing technologists. Visit MarTechConf.com for details.

LEARN MORE ABOUT OUR MARTECH EVENTS

WHITE PAPERS

- Why You Need To Be A Modern Marketer
- Marketer's Guide to Call Tracking for Local Search
- The Q4 2014 Performance Marketer's Benchmark Report

SEE ALL

WEBCASTS

- What's That Smell? Your R.O.T. Content
- Writing Ad Copy That Converts
- Click-to-Call Deep Dive: Best Practices from Search Experts

SEE ALL

RESEARCH REPORTS

- Enterprise Paid Media Campaign Management Platforms 2015: A Marketer's Report
- B2B Marketing Automation Platforms 2015: A Marketer's Guide
- Content Marketing Tools 2015: A Marketer's Guide
- Enterprise Social Media Management Software 2014: A Marketer's Guide

SEE ALL

Sign up for our daily newsletter.

Enter your email here.

Marketing Land Search Engine Land

FB000000351

Channels

- CMO
- Social
- Search
- Mobile
- Analytics
- MarTech
- Display
- Email
- Retail
- Content
- Video
- Local
- Industry

About

- About Us
- Contact
- Privacy
- Advertise
- Staff
- Connect With Us

Follow Us

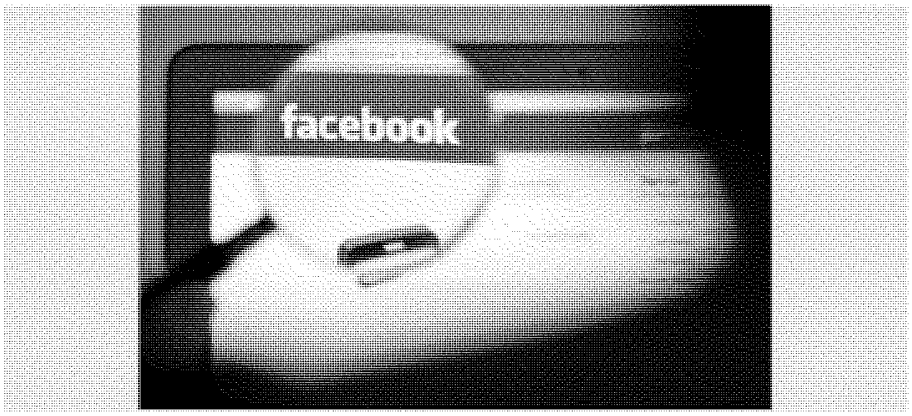
- Facebook
- Twitter
- Google +
- Tumblr
- LinkedIn
- Pinterest
- Youtube
- Instagram
- Newsletters
- RSS

Technology | Thu Jul 12, 2012 1:56am EDT

Related: U.S., TECH, MEDIA, FACEBOOK

Social networks scan for sexual predators, with uneven results

SAN FRANCISCO | BY JOSEPH MENN



In this photo illustration, a Facebook logo on a computer screen is seen through a magnifying glass held by a woman in Bern May 19, 2012.
REUTERS/THOMAS HODEL

(Reuters) - On March 9 of this year, a piece of Facebook software spotted something suspicious.

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.

Facebook is among the many companies that are embracing a combination of new technologies and human monitoring to thwart sex predators. Such 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.

Yet even though defensive techniques are now available and effective they can be expensive. They can also alienate some of a site's target audience -- especially teen users who expect more freedom of expression. While many top sites catering to young children are quite vigilant, the same can't be said for the burgeoning array of online options for the

TRENDING ON REUTERS

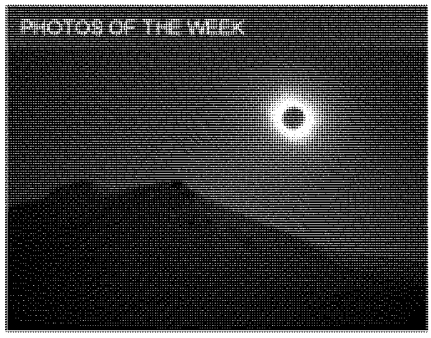
1 Torn-up sick notes show crash pilot should have been grounded | VIDEO

2 Apple's Tim Cook will give away all his money: Fortune

3 Germanwings co-pilot had serious depressive episode: Bild newspaper | VIDEO

4 Co-pilot suspected of deliberately crashing Germanwings jet | VIDEO

5 Police seek two people reportedly missing after New York explosion | VIDEO



Our top news photography of the week. Slideshow »

Editor's Choice

Building collapse in New York

Wreckage in the Alps

Air strikes on Yemen

In the land of Boko Haram

13- to 18-year-old set.

"There are companies out there that are doing a very good job, working within the confines of what they have available," said Brooke Donahue, a supervisory special agent with an FBI team devoted to Internet predators and child pornography. "There are companies out there that are more concerned about profitability."

RELATED COVERAGE

› FACT BOX: Expert advice to keep kids safe online

THE SMARTPHONE FACTOR

Two recent incidents are raising new questions about companies' willingness to invest in safety.

Last month the maker of a smartphone app called Skout, designed for flirtation with strangers in the same area, admitted its use had led to sexual assaults on three teenagers by adults. The venture-backed firm had not verified that users of its now-shuttered teen section were under 20, giving predators easy access.

Also in June, a teen-oriented virtual world called Habbo Hotel, which boasts hundreds of millions of registered users, temporarily blocked all chatting after UK television reported that two sex predators had found victims on the site and that a journalist posing as an 11-year-old girl was bombarded with explicit remarks and requests that she disrobe on webcam.

Former employees said site owner Sulake of Finland laid off many in-house workers earlier this year, leaving it unable to moderate 70 million lines of daily chat adequately. Sulake said it had kept 225 moderators and is still investigating what went wrong.

The failures at Skout and Habbo shocked child-safety experts and technology professionals, who fear they will lead to a renewed panic about online safety that is not justified by the data.

By some measures, Internet-related sex crimes against children have always been rare and are now falling (as are reports of assaults on minors that do not involve the Net). Most sex crimes against children are committed by people the children know, rather than strangers.

The National Center for Missing and Exploited Children processed 3,638 reports of online "enticement" of children by adults last year, down from 4,053 in 2010 and 5,759 in 2009.

Even those companies with state-of-the-art defenses spend far more time trying to stop online bullying and attempts to sneak profanity past automatic word filters than they do fending off sex predators.

Still, as the Skout case showed, there are several recent trends that have heightened the concerns of child-safety experts: the rise of smartphones, which are harder for parents to monitor; location-oriented services, which are the darling of Net companies seeking more ad revenue from local businesses; and the rapid proliferation in phone and tablet apps, which don't always make clear what data they are using and distributing.

EXPENSIVE DEFENSES

A solid system for defending against online predators requires both oversight by trained

employees and intelligent software that not only searches for improper communication but also analyzes patterns of behavior, experts said.

The better software typically starts as a filter, blocking the exchange of abusive language and personal contact information such as email addresses, phone numbers and Skype login names. But instead of looking just at one set of messages it will 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.

Companies can set the software to take many defensive steps automatically, including temporarily silencing those who are breaking rules or banning them permanently. As a result, many threats are eliminated without human intervention and moderators at the company are notified later.

Sites that operate with such software still should have one professional on safety patrol for every 2,000 users online at the same time, said Sacramento-based Metaverse Mod Squad, a moderating service. At that level the human side of the task entails "months and months of boredom followed by a few minutes of your hair on fire," said Metaverse Vice President Rich Weil.

Metaverse uses hundreds of employees and contractors to monitor websites for clients including virtual world Second Life, Time Warner's Warner Brothers and the PBS public television service.

Metaverse Chief Executive Amy Pritchard said that in five years her staff only intercepted something terrifying once, about a month ago, when a man on a discussion board for a major media company was asking for the email address of a young site user.

Software recognized that the same person had been making similar requests of others and flagged the account for Metaverse moderators. They called the media company, which then alerted authorities. Other sites aimed at kids agree that such crises are rarities.

NAUGHTY USERS, NICER REVENUES

Sites aimed at those under 13 are very different from those with large teen audiences.

Under a 1998 law known as COPPA, for the Children's Online Privacy Protection Act, sites directed at those 12 and under must have verified parental consent before collecting data on children. Some sites go much further: Disney's Club Penguin offers a choice of viewing either filtered chat that avoids blacklisted words or chats that contain only words that the company has pre-approved.

Filters and moderators are essential for a clean experience, said Claire Quinn, safety chief at a smaller site aimed at kids and young teens, WeeWorld. But the programs and people cost money and can depress ad rates.

"You might lose some of your naughty users, and if you lose traffic you might lose some of your revenue," Quinn said. "You have to be prepared to take a hit."

There is no legal or technical reason that companies with large teen audiences, like Facebook, or mainly teen users, such as Habbo, can't do the same thing as Disney and WeeWorld.

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.

The looser the filters, the more the need for the most sophisticated monitoring tools, like those employed at Facebook and those offered by independent companies such as the UK's Crisp Thinking, which works for Lego, Electronic Arts, and Sony Corp's online entertainment unit, among others.

In addition to blocking forbidden words and strings of digits that could represent phone numbers, Crisp assigns warning scores to chats based on multiple categories of information, including the use of profanity, personally identifying information and signs of grooming. Things like too many "unrequited" messages, or those that go unresponded to, also factor in, because they correlate with spamming or attempts to groom in quantity, as does analysis of the actual chats of convicted pedophiles.

The highest scores generate color-coded "tickets," with those marked red requiring the quickest response from moderators.

Facebook's software likewise depends on relationship analysis and archives of real chats that preceded sex assaults, Chief Security Officer Joe Sullivan told Reuters in the company's most expansive comments on the subject to date.

Like most of its peers, Facebook generally avoids discussing its safety practices to discourage scare stories, because it doesn't catch many wrongdoers, and to sidestep privacy concerns. Users could be unnerved about the extent to which their conversations are reviewed, at least by computer programs.

CATCHING ONE IN 10?

In part because of its massive size, Facebook relies more than some rivals on such technology.

"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. In addition, Facebook doesn't probe deeply into what it thinks are pre-existing relationships.

A low rate of false positives, though, also means that many dangerous communications go undetected.

Some adults have used Facebook to target dozens of minors before assaulting one or more and then being identified by their victims or the victims' parents, court records show.

"I feel for every one we arrest, ten others get through the system," Florida's Duncan said of tips from Facebook and other companies.

Another pillar in Facebook's strategy is to limit how those under 18 can interact on the site and to make it harder for adults to find them. Minors don't show up in public searches, only friends of friends can send them Facebook messages, and only friends can chat with them.

The gaping hole in the defense of Facebook and many other sites popular with teens is that minors can easily make up a birth date and pretend to be adults -- and adults can pretend to be minors, as happened with Skout, which declined an interview request.

Technology is available for verifying the ages of Web and app users. One of the providers is Aristotle International Inc, which offers a variety of methods, including having a parent vouch for a child and make a token payment with a credit card to establish the parent's identity.

Yet even in the wake of the Skout disaster, no site aimed at minors has hired Aristotle for

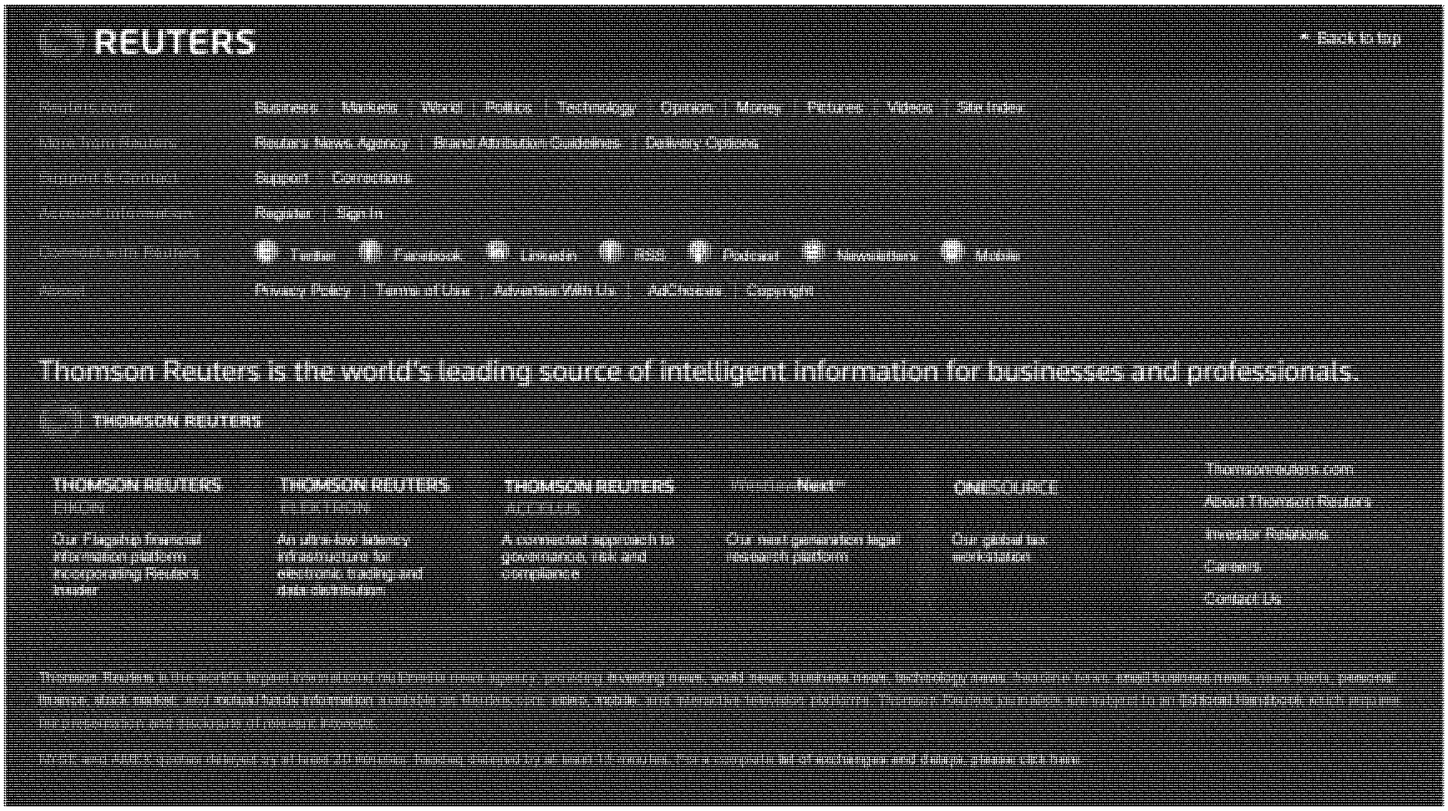
age checks. "We could do real parental consent with 14-year-olds, but no one has asked," said Aristotle Chief Executive John Phillips.

Such checks would cost money and alienate teens who don't want their parents involved.

Barring a wave of costly litigation or new laws, it is hard to see the protections getting much tougher, experts said. Instead, the app and location booms will only add to the market pressure for more freedom on youth sites and greater challenges for parents.

"For every Skout that shuts down, there are ten more that popped up yesterday," said the FBI's Donahue. "The free market pushes towards permissiveness."

(Editing by Jonathan Weber and Prudence Crowther)



Facebook Monitors Your Posts and Chats To Catch Sexual Predators

By Will Oremus

A poster is seen below a message board announcing Facebook's IPO price in Times Square in New York City on May 17.

Photo by Justin Sullivan/Getty Images

Ever wonder if Facebook is reading your posts? Well, it is—or, its computers are, at least. A if you say the wrong thing, you could be locked up.

WILL OREMUS

Will Oremus is *Slate*'s senior technology writer. Email him atwill.oremus@slate.com or follow hi on Twitter.

That's the takeaway from a recent Reuters article, which recounted a case in

with a 13-year-old Florida girl for sex. From Reuters:

> 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.

Facebook's chief security officer told Reuters that the company's monitoring software uses actual chats that led to sexual assaults to predict when another might occur. This is eerily similar to the hypothetical software I discussed in an article last month on whether police could arrest people based on suspicious-looking Google searches. I noted in the piece th while the idea might sound far-fetched, the technology already exists, and it might even be legal.

In Facebook's case, the scanning hasn't stirred outrage—probably because it seems to be focused on catching sexual predators. There are two reasons why online predators make sen as an initial target for automatic-monitoring algorithms. First, soliciting sex with a minor or the Internet is a crime in itself, not just a prelude to a crime (like, say, searching Google for ways to murder someone in their sleep). And second, sexual predators are unlikely to elicit much sympathy, so the public is more likely to tolerate intrusive means of nabbing them. Facebook is fighting creepy with creepy.

The key to the technology's success—from a public-opinion standpoint, and possibly from legal standpoint—is avoiding false positives. Arresting an innocent person based on a Facebook chat would surely cause controversy. So according to the Reuters piece, Faceboo dials down the algorithm's sensitivity, to minimize the chances of this happening.

It seems clear that this technology has the potential to do some good. But that shouldn't blir us to the fact that it represents a further erosion of our online privacy, one more serious thar selling our personal information to advertisers.

Future Tense is a partnership of Slate, New America, and Arizona State University.

THE VERGE

Facebook analyzes relationships and chats to flag up sexual predators

By louisgoddard on July 13, 2012 06:05 am

Facebook automatically scans posts and chat logs for criminal activity, using big data processing techniques similar to those used in targeting advertising to determine the most vulnerable users, according to a new *Reuters* report that explores combating pedophilia in social media. The social network's scanning tools use factors such as mutual friends, past interaction, distance and age difference — alongside simple phrase searches — to flag potentially nefarious

conversations for human moderators. They also rely on archives of previous conversations that are known to have led to sexual assaults, identifying patterns and searching for similar ones.

> *"WE USE TECHNOLOGY THAT HAS A VERY LOW FALSE-POSITIVE RATE."*

Apparently keen to pre-empt the sorts of privacy concerns that have dogged Facebook in recent months, Chief Security Officer Joe Sullivan tells *Reuters* that "it's really important that we use technology that has a very low false-positive rate." He explains that "[w]e've never wanted to set up an environment where we have employees looking at private communications," stressing that the company's systems attempt to avoid flagging up long-standing personal relationships. A lot of the activity that Facebook refers to law enforcement is identified through its user reporting system, detailed in a recent infographic.

Privacy issues aside, it would be practically impossible for human moderators to effectively trawl through the vast amount of data generated by more than 900 million users each day. Even much smaller sites such as Habbo Hotel are unable to provide effective human monitoring — lacking Facebook's automatic flagging technology, the site became embroiled in an embarrassing pedophile scandal last month, when a journalist posing as a 13-year-old girl was bombarded with sexually explicit messages.

Facebook limits interactions with under-18s, removing their profiles from public searches while restricting messaging to friends-of-friends and chat to friends only. Unfortunately, this doesn't solve the issue of users providing false ages, a problem which cuts both ways: while predatory adults are known to impersonate teens, children younger than 13 also frequently lie about their age to gain access to the site.

Facebook scans chats and posts for criminal activity

Facebook's monitoring software focuses on conversations between members who have a loose relationship on the social network.

by Emil Protalinski @emilprotalinski / July 12, 2012 5:45 PM PDT

Facebook has added sleuthing to its array of data-mining capabilities, scanning your posts and chats for criminal activity. If the social-networking giant detects suspicious behavior, it flags the content and determines if further steps, such as informing the police, are required.

The new tidbit about the company's monitoring system comes from a Reuters interview with Facebook Chief Security Officer Joe Sullivan. Here's the lead-in to the Reuters story:

> 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. 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.

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.

"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," Sullivan told Reuters. While details of the tool are still scarce, it's a well-known fact that Facebook cooperates with the police, since, like any company, it has to abide by the law. In fact, just a few months ago, Facebook complied with a police subpoena by sending over 62 pages of photos, Wall posts, messages, contacts, and past activity on the site for a murder suspect.

For more information about Facebook's stance on working with the police, I

THIS WEEK'S MUST READS /

1 Facebook scans chats and posts for criminal activity
Internet

2 Samsung bets big on April 10 launch of Galaxy S6, S6 Edge
Mobile

3 BlackBerry shows signs of life, posts surprise quarterly profit
Mobile

4 Apple's Tim Cook plans to donate his wealth to charity
Tech Industry

5 Intel, Micron, Toshiba promise storage that's fast and roomy
Computers

checked out these two pages: Law Enforcement and Third-Party Matters, as well as Information for Law Enforcement Authorities. It's worth noting that neither of these documents discusses the aforementioned tool (a quick search for the words "monitor" and "scan" bring up nothing).

Facebook likely wants to avoid discussing the existence of the monitoring technology in order to avoid further privacy concerns. Many users don't like the idea of having their conversations reviewed, even if it's done by software and rarely by Facebook employees.

See also:

Here's what Facebook sends the cops in response to a subpoena
Mark Zuckerberg: Facebook users eventually get over privacy anxiety
Facebook CTO: most people have modified their privacy settings
Facebook settles with FTC over default privacy settings
Survey: Facebook, Google privacy policies are incomprehensible
How to protect your Facebook Timeline privacy
Low voter turnout means new Facebook privacy policy wins

Tags: Internet, Privacy, Mark Zuckerberg, Facebook

ABOUT THE AUTHOR

Emil Protalinski / 
Emil is a freelance journalist writing for CNET and ZDNet. Over the years, he has covered the tech industry for multiple publications, including Ars Technica, Neowin, and TechSpot. See full bio

DISCUSS FACEBOOK SCANS CHATS AND POSTS FOR CRIMINAL ACTIVITY

Show Comments

LATEST ARTICLES FROM CNET

Cyclist's helmet-cam video of argument with driver shows glory of humanity

Google loses ruling in Safari tracking case

Comedian Will Ferrell belts out 'Star Trek' theme

HTC's smartphone design chief hangs it up

Get Sol Republic Tracks Air Bluetooth headphones for $74.95

REVIEWS
All Reviews
Audio
Cameras
Car Tech
Desktops
Laptops
Phones
Tablets
TVs

NEWS
All News
Apple
Crave
Internet
Microsoft
Mobile
Sci-Tech
Security
Tech Industry

VIDEO
All Video
Apple Byte
CNET On Cars
CNET Top 5
CNET Update
Next Big Thing
The 404
The Fix
XCAR

MORE
About CBS Interactive
About CNET
CNET 100
CNET Deals
CNET Forums
CNET Magazine
CNET Mobile
Help Center
Permissions

FOLLOW CNET VIA...
Facebook
Twitter
Google+
YouTube
LinkedIn
Tumblr
Pinterest
Newsletters
RSS

Mashable

Facebook Monitors Your Chats for Criminal Activity [REPORT]

50.5k
Share on Facebook Share Tweet on Twitter Share Share

BY ALEX FITZPATRICK
JUL. 12, 2012

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 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.

Keeping most of the scanned chats out of the eyes of Facebook employees may help Facebook deflect criticism from privacy advocates, but whether the scanned chats are deleted or stored permanently is yet unknown.

The new details about Facebook's monitoring system came from an interview which the company's Chief Security Officer Joe Sullivan gave to Reuters. At least one alleged child predator has been brought to trial directly as a result of Facebook's chat scanning, according to Reuters' report.

When asked for a comment, Facebook only repeated the remarks given by Sullivan to 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."

SEE ALSO: State Law Requires Sex Offenders to List Status on Facebook

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."

Indeed, Facebook has cooperated with police investigations in the past. In April, it complied with a police subpoena from the Boston Police Department by sending printouts of wall posts, photos and login/IP data of a murder suspect.

Is Facebook doing a public service by monitoring chats for criminal behavior? Share your thoughts in the comments.

Image courtesy of iStockphoto, adventtr

TOPICS: CENSORSHIP, FACEBOOK, PRIVACY, SECURITY, SOCIAL MEDIA

Business

Tim Cook will give away his Apple fortune

Lance Ulanoff

Apple's CEO will donate his money to charity before he dies. A bold move that may or may not have Steve Jobs rolling over in his grave.

1.4k shares 1 hour ago
Share Tweet Share Share

World

'This is about to get real': NASA twin astronaut prepares for a year in space

Andrew Freedman

NASA astronaut Scott Kelly is set to launch on a yearlong mission to the International Space Station on Friday that will also involve his twin brother, Mark.

751 shares 2 hours ago
Share Tweet Share Share

Watercooler

Mom proudly shares her stretch marks in viral bikini photo

Laura Vitto

The photo of Hollis smiling wide while dressed in a bikini, and its corresponding caption, has been Liked more than 400,000 times, and shared more than 50,000 times.

1.4k shares 2 hours ago
Share Tweet Share Share

Watercooler

Woman gets Instagram to accept periods are normal after her photo is removed twice

Andrea Romano

Periods are normal for women, whether Instagram wants to see it or not.

2.7k shares 3 hours ago
Share Tweet Share Share

Entertainment

Meerkat and Periscope for concerts? Katy Perry says 'embrace the future'

Brian Anthony Hernandez

"You've got to embrace the future or you're left behind," Katy Perry told 'Mashable.' "I think that, when you see a phone, that is like the new applause."

Travel

Hiker's incredible transformation captured in selfies over 2,600 mile journey

Max Knoblauch

The change in the landscape, scenery and Davidhazy's weight and facial hair are incredible to watch.

More in Social Media

NEW

What's New

What's Rising

What's Hot

Your Facebook Chats Are Being Monitored, By Facebook

DOUG MATACONIS · FRIDAY, JULY 13, 2012 · 5 COMMENTS

Mashable is out with a report that **Facebook routinely monitors user chats for suspicious or 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 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.
>
> Keeping most of the scanned chats out of the eyes of Facebook employees may help Facebook deflect criticism from privacy advocates, but whether the scanned chats are deleted or stored permanently is yet unknown.

The news was first broken in a Reuters story that **describes one incident in which the software did in fact catch a child predator:**

> (Reuters) – On March 9 of this year, a piece of Facebook software spotted

> something suspicious.
>
> 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.
>
> Facebook is among the many companies that are embracing a combination of new technologies and human monitoring to thwart sex predators. Such 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.

As it turns out, this is all covered in the company's **Privacy Policies:**

> "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."

It's hard to argue with what Facebook is doing here. Yes, there are some privacy concerns here, but Facebook is a private company and free to set its own policies on these issues. Additionally, it has a corporate brand to protect, not to mention the potential of liability, from being known as a place where parents can't be sure that their teenager children can be safe. Of course, one should also point out that parents should probably be more vigilant about keeping an eye on what their kids are doing online, especially when it is so easy for them to manipulate Facebook's settings to make it appear like they are older than they actually are.

FILED UNDER: **DOUG MATACONIS, ECONOMICS AND BUSINESS, QUICK PICKS, SCIENCE & TECHNOLOGY, FACEBOOK, PRIVACY**

Related Posts:

Facebook Privacy Tip

A Question for Lawyers in the Audience (Social Media and Employees)

Facebook Adds Gay Friendly Status Options

Want A Job: Give Us Your Facebook Password

About Doug Mataconis

Doug holds a B.A. in Political Science from Rutgers University and J.D. from George Mason University School of Law. He joined the staff of OTB in May, 2010 and also writes at **Below The Beltway**. Follow Doug on **Twitter** | **Facebook**

Comments

Franklin says:
Friday, July 13, 2012 at 09:26

At this point, there's really no reason for Facebook users to expect any privacy. Which is one of many reasons I don't use it.

Like or Dislike: 9 0

Ben says:
Friday, July 13, 2012 at 09:55

That privacy policy doesn't say anything about monitoring correspondence. All it says is that it will share information and respond to subpoenas. I don't think you could reasonably construe that privacy policy to say "we're monitoring everything you're doing and saying."

Like or Dislike: 4 0

bandit says:
Friday, July 13, 2012 at 11:48

Reality is that they have a transaction record of every message and they have it stored and available – 'monitoring' is probably reporting on key words – I think there's more than enough evidence that they're entirely good with passing this data along.

Like or Dislike: 3 0

al-Ameda says:
Friday, July 13, 2012 at 13:18

I know many young people who have significantly cut back their use of Facebook – they felt that they were ceding too much of their privacy to Facebook.

My youngest daughter (mid-twenties) says that Microsoft is the Evil Empire, Apple

is a Cult, and Facebook makes life difficult.

Like or Dislike: 4 0

Phillip says:
Friday, July 13, 2012 at 19:20

Ah, the joys of having never joined Facebook!

Like or Dislike: 3 0

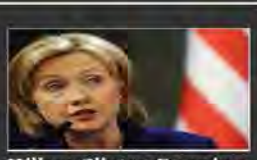
EDITOR'S PICKS

Ted Cruz And The Question Of When A Candidate Is "Qualified" To Be President

Indiana To Give Religious Business Owners The Right To Discriminate Against Gays

Yes, Ted Cruz Is A "Natural Born Citizen"

President Obama Supports Mandatory Voting, And He's Wrong To Do So



Hillary Clinton Running Away with the Race

About
Archives
Policies
Privacy
Disclosures
Contact
Sitemap

US Politics
- Borders & Immigration
- Campaign 2012
- Congress
- Public Opinion Polls

World Politics
- Africa
- Asia
- Europe
- Latin America
- Middle East
- United Nations

National Security
- Intelligence
- Military Affairs
- Terrorism

Entertainment
- Contests
- Humor
- Late Night OTB
- Popular Culture
- Sports

Business & Economics
Gender Issues
Law & the Courts
Media
Race & Politics
Religion
Science & Technology
Best of OTB

↑ Top ↑

FB000000375

nakedsecurity
Award-winning computer security news from SOPHOS

How Facebook catches would-be child molesters by analyzing relationships and chat content

by Lisa Vaas on July 16, 2012 | 33 Comments
FILED UNDER: Facebook, Law & order, Privacy, Social networks

Law enforcement is hailing Facebook for using its little-known data monitoring technology to spot a suspicious conversation about sex between a man in his early thirties and a 13-year-old girl from Florida.

According to Reuters, Facebook software on March 9 raised the red flag when it picked up on a conversation about sex between the man and the girl.

The two had only a loose relationship on the network.

The man was chatting about sex with the girl and planned to meet her after middle-school classes the next day, according to Reuters.

The conversation was automatically flagged for Facebook employees, who read it and quickly notified the police.

Police took over the girl's computer and arrested the man the following day, Special Agent Supervisor Jeffrey Duncan of the Florida Department of Law Enforcement told Reuters.

The alleged predator has pleaded not guilty to charges of soliciting a minor.

Facebook doesn't talk much about this technology, which scans postings and chats for criminal activity.

In what Reuters called the company's "most expansive comments on the subject to date", Facebook Chief Security Officer Joe Sullivan said that the monitoring software analyzes relationships to find suspicious conversations between unlikely pairings, i.e., between people of widely varying ages who only have loose and/or newly formed relationships, for example.

The technology also relies on archives of real-life chats that preceded sexual assaults, Sullivan told Reuters.

It's easy to see why Facebook doesn't talk about it much: the last thing the company wants is for its users to feel like they're being eavesdropped on, 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.

To avoid coming off as eavesdroppers, Facebook also avoids probing what it interprets as pre-existing relationships, Sullivan said.

Reining in its monitoring technology is understandable in light of not wanting to be

perceived as Big Brother, but as Reuters pointed out, a low false-positive rate has the serious downside of letting many dangerous communications go through unflagged.

Duncan estimates that for every predator the police intercept due to tips from Facebook and other companies, another ten get through the system undetected.

And while Facebook limits how visible children are to its adult users - minors don't show up in public searches, only friends can chat with them, and only friends' friends can send them messages - children are all too capable of lying about their age and pretending to be adults.

The converse is true: adults can lie about their birth dates and pretend to be minors.

One example can be found in Skout, a location-based social networking mobile app and website that in June barred minors from using its service, following three separate incidents in which children were allegedly sexually assaulted by adults posing as teenagers.

At the time, the New York Times reported that Skout was fully aware that minors were using its site.

Skout had, in fact, put safeguards in place to protect those minors. Last year, after noticing minors using its service, Skout put together a separate service for 13- to 17-year-olds with safety features such as parental controls.

In addition, Skout devoted a quarter of its staff to monitoring activity to flag nudity, and to check chats for inappropriate sexual messages, profanity, spamming, copyright infringement and violent behavior. The service also banned tens of thousands of infringing devices every month.

In spite of Skout's efforts, three children were allegedly targeted, raped or molested.

There's no lack of security to protect against the type of age falsification that creates problems on Facebook and sites such as Skout.

Reuters pointed to one such provider, Aristotle International Inc., which offers methods such as having a parent vouch for a child with a token credit card payment.

The problem is, nobody's buying.

The downsides of such technology: it bleeds away sites' profits because it costs money, and it drives away children who crave unfettered freedom of communication.

Children's natural development includes the need to break away from their families as they seek independence.

Tragically, there are no end of online venues that have the look and feel of sanctuaries where it's safe to do that in the presence of peers.

It's crucial to somehow get through to them that those sanctuaries can be smoke and mirrors, and that those supposed peers can all too easily be dangerous predators.

Parents, law enforcement, you have my sympathy. The task seems overwhelmingly daunting.

How do you get these lessons through to minors? Please, share your wisdom with us by leaving a comment below.

If you want to learn more about privacy and security threats on the social network and elsewhere on the internet, join the **Sophos Facebook page**.

Fingers at keyboard and Child at computer images courtesy of Shutterstock.

Tags: child abuse, child predators, data analysis, data mining, Facebook, Privacy, Skout

How likely are you to recommend Naked Security to a friend or colleague?

0 1 2 3 4 5 6 7 8 9 10

Vote

You might like

Child abuser sues Facebook and page admin over allegedly posting his address

Justin Bieber imposter jailed after tricking children into stripping in front of webcam

Facebook scans private messages to inflate the "Like" counter on websites

Convicted sex offenders must reveal their criminal status on Facebook, says Louisiana law

33 Responses to *How Facebook catches would-be child molesters by analyzing relationships and chat content*

Richard · 984 days ago

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

Yeah, let's flag *every* conversation for monitoring, just in case.

Malo periculosam, libertatem quam quietam servitutem.

1 2 Rate This

Reply

@Otaku2012 · 984 days ago

Kudo's to Facebook on finally doing the right thing. Next, try fixing that crappy strict TOS so they are more clear and hire competent admin.

1 1 Rate This

Reply

Madelin Farfan · 980 days ago

"Kudos" my ass.... Just wait until YOU are on the receiving end of that "right thing". Don't think it can't happen, because you're a bigger fool than I thought . 'Big Brother' (i.e.) Police State totalitarian tactics, are now in full force. STOP giving "law enforcement" any more power than they already have!

1 2 Rate This

Reply

Joe Hayhurst · 984 days ago

Thin end of the wedge. I suppose it's reassuring in one respect that Facebook are trying to prevent child exploitation, but it's no stretch to imagine law enforcement, security services etc now working with Facebook to try and detect all sorts of

other crimes - I probably would if I was the police.

Everyone now has to assume you have absolutely ZERO privacy on the web unless you are using a full secured and encrypted system that you have personally set up and understand. If you're using someone else's system, forget it.

1 1 Rate This

Reply

Mike · 984 days ago

Ok. Why was a 13 year old on Facebook, unsupervised?

0 0 Rate This

Reply

Machin Shin · 984 days ago

Ok, What are the odds you could keep a determined 13 year old off facebook if they wanted to be? I would be willing to bet a very large sum of money on the 13 year olds ability to get around anything you did to try and stop or monitor them.

Does not mean should do nothing but really do need to wake up and realize you can't keep a kid in a little "perfect world bubble".

0 0 Rate This

Reply

Lisa Vaas · 984 days ago

Do you honestly think you can monitor a 13-year-old 24x7?

2 1 Rate This

Reply

Dutchology · 984 days ago

My mother monitors a perfectly happy, well socialised 16 year old girl. She holds the password to her Facebook page whereas the 16 year old doesn't. She controls computer time in a public area of the house and that 16 year old is happy to use Facebook in this manner. She doesn't rebel against it and is not secretly holding an account elsewhere, she doesn't feel the need to. She's rarely on Facebook and just uses it to catch up with friends on weekends or during school holidays. I can't see the problem.

0 0 Rate This

Reply

jdclover · 984 days ago

How does one guarantee that that is the only facebook account? Although it's against the facebook TOS, I know people that have more than one account, one for friends and one for family or business. I'm sure a teen could easily do this as well.

1 0 Rate This

Reply

Yadont · 983 days ago

"I can't see the problem."

The problem is not everybody lives in Mayberry. Not every parent has written a GIAC gold paper on properly securing a home network and not every kid is a perfectly compliant little angel who wouldn't dream of circumventing any restrictions you place on them. Many of those non-angels are better at getting around controls than their parents are at implementing them.

3 0 Rate This

Reply

Freida Gray · 983 days ago

Facebook allows 13 year old children to set up an account.Thirteen is the minimum age for an account stated in Facebook's TOS.

0 0 Rate This

Reply

Xyon · 984 days ago

As a parent of young children the openness of the web terrifies me as a concept for them when they reach ages that they'll start using services like facebook (or whatever is the flavour of the month at the time). As an IT professional, I set up dansguardian on the home network as a means to protect our home traffic from this kind of thing - but that's only one connection. 4G wireless, school, friends' internet, I can't monitor...

0 0 Rate This

Reply

Lisa Vaas · 983 days ago

I think you've nailed the main problem with trying to institute constant monitoring of minors' usage: networks are ubiquitous. A parent well may be able to keep an eye on a child's at-home Internet activity, but can that parent really be expected to stay on top of Internet activity when their child's messing around with smartphones, with school networks, with friends' home networks, at wifi hotspots, and/or at libraries' networks?

It's when the child's outside of parental monitoring that you have to rely on having educated the kid well enough that they know better than to trust somebody they met on Facebook.

I'm loathe to blame parents even when kids fall into traps, though. Their brains aren't fully developed. They're easy targets for extremely sophisticated predation. Hell, we all are, let's face it. Some guy flashed a badge at me and a traveling companion in Athens years ago, then asked to see our wallets to determine if a supposed pickpocket had managed to rob us. We, being gullible, law-abiding citizens, gave him our wallets. Luckily, he handed them back, since they had so little cash. It was after he asked to see our "secret, hidden" money that I smelled a rat and asked to see his badge again.

It turned out to be a toy plastic badge.

People are easy to fool. Children are magnitudes easier.

1 1 Rate This

Reply

sharp · 982 days ago

It just requires giving them the tool that you will monitor.
The difference I see, is that parents confront the children, which causes them to distrust their parents more for spying on them.

I believe there is a difference between monitoring and being there, over contronting an issue instead of keeping the child safe and allowing them to learn from their own mistakes.

These other places you refer to are mostly monitored locations that prohibit certain things. (School, Library, phones). I believe the Schools block facebook, library requires parent permission, and Cell phones need paid. It's not like it requires much for an IT to pull logs and hand them to parents, and say here is the data it's yours to monitor through, unless your paying for monitoring. This is what the phone company does, hands you the logs and leaves it to the parents to investigate.

0 0 Rate This

Reply

Darlene Wigston · 984 days ago

I have nothing to hide and am glad to see this (not that those who want to protect their privacy have something to hide -- I know they generally don't -- but those who do have something to hide will lie and say it's about privacy). I don't care if Facebook knows I made cupcakes last night. But I do care if no one knows if a child is about to be molested.

1 0 Rate This

Reply

Simon McAllister · 984 days ago

Well said! Being a parent myself, I too would like as much support, particularly when the said social network has millions of accounts; not all 'real' users. One day I would expect to see some sort of verification for an account so that it's impossible to setup a 'fake' user. See what difference that would make....

1 0 Rate This

Reply

Judy K. · 984 days ago

"I don't care if Facebook knows I made cupcakes last night. But I do care if no one knows if a child is about to be molested." It's this mentality that got us here in the first place. Rather than deal with criminals when we're supposed to, we'd rather give up our freedoms in the name of security. This person has pleaded "not guilty", no surprise there, and he'll probably get off on some stupid premise that he had too much coffee that day. Then, not only will he be able to continue doing what he's doing, we'll agree to give up that much more freedom to protect our children from him. He should be dealt with now. And since this is about minors, parents have to bite the bullet and be firm with their children about what

they can and can not do. You're not your child's friend, you're their parent. And they don't need full autonomy prior to the age of majority and with the way many of these kids are growing up, not even then.

0 1 Rate This

Reply

John · 945 days ago

I grew up with facebook and am currently 24. i have read quite a bit about how personalities and thought processes develop. In my experience and research supported opinion the 13y/os looking to befriend or lose their virginity to way older men(or women) generally have parents that are guilty of emotional abuse....not as you claim "trying to be their friend"

the problem is compounded by the slave like work hours many middle class and all lower class parents face. it is even further compounded if the parent actually has a personality disorder or hates the situation and avoids the family then feels guilty and trys to parent the child by "being the adult not the friend" and picking out something to try to improve on the child by discipline....they tune into the teens life for a moment and based on that single moment disconnected from any knowledge of what led up to it or even what the teen was intending to do....they decide the teen is a child, on a bad track and needs to be punished.... the parents i am describing then often fail to tune in and notice good things or provide emotional support for hard times.

what that reaction communicates to the child is: i dont care enough to listen to the full story. you are incapable of doing things for yourself and you are a bad person.

the above can cause many outcomes. a very common one happens to be the desire to be desired.... and the desire to find an elder that can fill the void left by negative, inattentive or emotionally abusive parents.

you cant be the friend all the time but focusing mainly on disciplined will probably screw your child up worse... BALANCE is the key. if you are going to be strict you need to be just as rewarding or you will create issues in your childs head.

all friend no parent tends to manifest in the house where kids get to party while the parents are there... or the house were the parents bought the booze for them.

if its the house where the parent doesnt pay attention to the kids partying it can create the seek an elder void but the strict version is far more common due to the boomers influence.

the main point of all of the above is that black and white will bite you in the ass...if you parent with it... it might bite two souls in the ass.

as an addon i think you need to do some research on how strict and usually unavoidable sentencing is in these cases. there are 18y/os in jail in some states because the parents of the 17y/o didnt like it. they will for ever carry the mark of molester because of a black and white law that didnt take into account that they were peers. there are also cases of 16 y/o's with various adults that tell the court it was their idea... they lied about their age...and or they had a fake... guess who still goes to jail based on the black and white statutory laws which take away the judges ability to make the punishment fit the actual crime

many are saved but almost as many are ruined.

0 0 Rate This

Reply

EPB · 984 days ago

Freedom is hard to gain and easy to lose. Many of our ancestors fought to gain this freedom for us and we have the burden to honor them by protecting it. Although most of us can agree on obvious exceptions, exercising those exceptions creates precedence that could be used to limit our freedoms beyond the acceptable. We are short-sighted beings by nature and need to be cautious allowing activity that could spread to infringe our core rights.

0 0 Rate This

Reply

@bosslady2898 · 983 days ago

This is very disconcerting to me...I don't mind catching child molesters, but what else are they flagging? Democrats? Republicans? ...Fascinating...

0 0 Rate This

Reply

chunter · 983 days ago

Education is the only answer. If you don't teach children to avoid trouble, you won't prevent crime, and still, things will slip through.

It doesn't matter how many children it will save, policing thought is never okay.

0 0 Rate This

Reply

anonymous coward · 983 days ago

Exactly! Draconian restrictions on computer use (or at least restrictions that the teenager will consider draconian) will work for a while, but without some education the kid will go around them as soon as they can figure out how. But the same rules that Facebook is applying can be explained to kids who are old enough to be on Facebook. Explain to them that, while reasonably rare, there is danger in people pretending to be something other than what they really are, and not all of them are nice people. Relationships can start virtual as long as they stay virtual and no physical location info is communicated.

0 0 Rate This

Reply

Robert Latimer · 983 days ago

If you can't be open and transparent, then go back into your "bubble" and stay offline!!!!

0 1 Rate This

Reply

melinda · 983 days ago

Parents need to monitor their children properly. Too many parents are off doing their own thing and quite ignorant of the windows they've opened by letting their kids have smart phones, especially.

0 0 Rate This

Reply

Sabbath · 983 days ago

This is good method but telling people they can't use a computer umonitored till exactly their 18th birthday is a bit much.... the more you restrict people the less educated they are and the more problems they'll get into. If your kid isn't in a bubble all their lives they're not gonna need to be treated like they are 10 at 16...just saying.

0 0 Rate This

Reply

Ken · 983 days ago

I apologize in advance for this post.
For those of you who are suggesting enacting more laws, or stating that only "bad" people have something to hide. Please move to a police state and leave my American freedoms alone. Obviously you do not care about your freedoms, and think that an all powerful government / corporation will protect you. I am unsure where your disillusionment began, but you are far too trusting, kind of like your children with predators.

If you believe your children are susceptible to child predators, then educate your children not to be. If you say they are too young to know any better, then teach them, help them to know better. The argument that I am seeing now is that since you are unable to monitor your own children, you expect someone else to monitor them for you. Raise and educate your children properly, and you should be able to avoid these conditions. Although I'm not saying that it will protect them from everything, it will help to protect them from some things.

As far as Facebook monitoring, I understand why they are monitoring, there is big money involved in the data they are collecting. I disagree with the fact that they are monitoring, but in the end, I signed up for their service, and I continue to use it even though I know what some of their practices are. That is my fault, but I made that choice. With that being said, if they were to increase their monitoring efforts, and start disclosing more information then I will quit using their service.

1 0 Rate This

Reply

Internaut · 982 days ago

Most of the comments, and the issue around child protection on the Internet assumes that a 13 year old today is the same as we were when we were 13. From the moment they can sit in front of the TV, to their fist sit-down at a computer, they pickup faster, and a lot more than we ever could at that age. Our parents taught us about safety and strangers. Kids were rarely alone, and when outside, usually in groups playing together. Now, they are called 'gangs' - even if they are just playing.

I'm 63 and therefore not young enough to know everything anymore. But I've been around long enough to see the changes of where we were, what we are doing, and where we may be very soon. Having worked with youth grades 4 to 6