

3/27/2015

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

# naked security

Award-winning computer security news from **SOPHOS**

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

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com

Do it!

Don't show me this again

by Lisa Vaas on July 16, 2012 | 33 Comments

FILED UNDER: Facebook, Law &amp; 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

<https://nakedsecurity.sophos.com/2012/07/16/facebook-child-molester/>

1/12

FB000000376

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 servitatem.

1 2 Rate This




 **@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




 **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



 **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



 Mike · 984 days ago

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

0 0 Rate This




 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




 Lisa Vaas · 984 days ago

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

2 1 Rate This



 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



 jdlover · 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



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



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



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



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



 **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 confronting 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



 **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




 **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



 **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



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



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



@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



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



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



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



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



**Sabbath** · 983 days ago

This is good method but telling people they can't use a computer unmonitored 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



**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



**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 first 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

# EXHIBIT K



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

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

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

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

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

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

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

i

0 0 Rate This



**Richard** · 982 days ago

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

0 0 Rate This



**Sum Guy** · 982 days ago

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

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

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

Our children need to be monitored, The misbehave in way that would shock most of us when we are not looking. This current generation or adults is pretty poorly mannered. monitoring them may help the quality of the next generation to become important adults.

Of course this wont fix our society but maybe it will increase the good to bad ratio.

0 1 Rate This

Reply

 Ken · 982 days ago


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

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

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

2 0 Rate This

Reply


 Tony · 981 days ago

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

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

0 0 Rate This

Reply

 oncefallendotcom · 980 days ago

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

2 0 Rate This

Reply

 Maxwell · 956 days ago

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

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



0 1 Rate This



About the author

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

View all posts by Lisa Vaas

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

Tags: Adobe, Android, Apple, data breach, date files, DNS, Encryption, Exploit, Facebook, General, Google, hacking, iPhone, IT, Malware, Microsoft, password, Patch, Patch Tuesday, phishing, Privacy, scam, Spam, Twitter, Video, vulnerability, web, web 2.0, www

Archives by month: March 2015 (109), February 2015 (103), January 2015 (109), December 2014 (80), November 2014 (87), October 2014 (54), September 2014 (95), August 2014 (90), July 2014 (108), June 2014 (97), May 2014 (101), April 2014 (98), March 2014 (99), February 2014 (89), [More](#)

Categories: Android (1187), Apple (545), Cookies (623), Cryptography (1,564), Default Service (507), File transfers (1110), Firefox (460), Google (2,382), Hacked (277), Internet Explorer (693), Java (361), Malware (6,281), Mobile (1,580), Patches/Checkups (229), Operating Systems (72), OSs (1,665), Phishing (664), Policies (841), Passwords (395), Scopes/Labs (2,185), Technologies (33), Video (165), Web Browsers (445), Windows (892), Windows/Mac (110)

Download some free tools: [Free anti-virus for your Mac](#) (Free antivirus that works simply and beautifully), [Free Android protection](#) (Free antivirus for all your Android devices), [More free tools](#)

Take a look at our products: [Endpoint](#), [Mobile](#), [Email](#), [Encryption](#), [Network](#), [Web](#). Try out our [free trials and demos](#)

Investigate the threats: [Virus and spyware analysis](#), [Threat Center](#), [Intruder Detection Labs](#)



# SecurityWatch

with Neil Rubenking



Search Security Watch

### Top Categories

SEE ALL »

### Trending Tags

- malware
- vulnerability
- antivirus
- patch
- Android
- firefox
- Apple

SEE ALL »

### Follow



### More Blogs

#### AppScout



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

#### Forward Thinking



Living With a Sturdy Samsung Galaxy Tab Active

## Facebook Scans Chats for Criminal Activity

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

By Fahmida Y. Rashid



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

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

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

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

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

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

### Protect Yourself

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

- **Friending Strangers** – Study after study have shown Facebook users accept friend requests from people they don't know. It's easy to lie on a profile, and criminals do it all the time on social networking sites. Sexual predators have pretended to be teenagers to talk to younger users on social networking sites. In a recent analysis, researchers from Barracuda Networks found several fake Facebook profiles using the exact same

## //STAY CONNECTED

Get Product Reviews, Deals, & the Latest News from PCMag

JOIN OUR EMAIL LIST SIGN UP

Plus, get a free copy of PCMag for your iPhone or iPad today.

Offer valid for new PCMag app downloads only. Subscribing to a newsletter indicates your consent to our [Terms of Use](#) and [Privacy Policy](#).

## //FEATURED PROGRAMS

**GET ORGANIZED**  
How to Clean Up Your Messy Digital Life

Reimagine your digital life, become happier & more productive, Get Organized.



photograph of an attractive woman as the main profile picture. Once a fake profile is added as a friend, that scammer has access to a tremendous amount of personal data. Screen them out beforehand.

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

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

**Crimes Against Minors Online Rare**

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

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

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

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

**Protect Children**

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

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

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



**Comments**  
blog comments powered by Disqus

ABOUT	CONNECT	ZIFF DAVIS SITES	SUBSCRIBE	SOCIAL
<a href="#">About Us</a>	<a href="#">Login</a>	<a href="#">AskMen</a>	<a href="#">PC/Mac</a>	Facebook

<a href="#">Site Map</a>	<a href="#">PCMag Digital Edition</a>	<a href="#">Computer Shopper</a>	<a href="#">Apple iOS</a>	 <a href="#">Twitter</a>
<a href="#">Privacy Policy</a>	<a href="#">Newsletters</a>	<a href="#">ExtremeTech</a>	<a href="#">Amazon Kindle</a>	 <a href="#">Pinterest</a>
<a href="#">Terms of Use</a>	<a href="#">RSS Feeds</a>	<a href="#">Geek</a>	<a href="#">B&amp;N Nook</a>	 <a href="#">Google+</a>
<a href="#">Advertise</a>	<a href="#">Encyclopedia</a>	<a href="#">IGN</a>	<a href="#">Google Android</a>	
	<a href="#">Contact Us</a>	<a href="#">TechBargains</a>	<a href="#">Sony Reader</a>	
		<a href="#">Toolbox</a>	<a href="#">Customer Service</a>	

 © 1996-2015 Ziff Davis, LLC. PCMag Digital Group 



# Facebook's Spying On You For a Good Cause

Written by **ADAM ESTES**

July 13, 2012 // 01:10 PM EST

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

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

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

pedophiles away from minors online. Said one special agent from Florida, "I feel for every one we arrest, ten others get through the system."

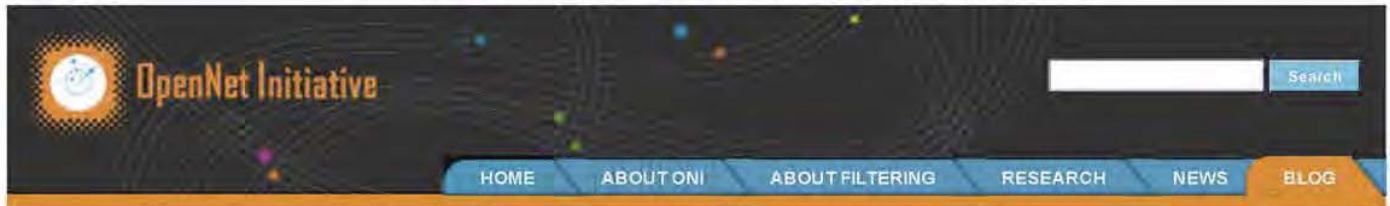
From the other side of the fence, though, it's easy to think of Facebook's anti-pedophile software as just another form of moderation. After all, Facebook employs an army of moderators to keep illicit photos from being uploaded, abusive language from being used in the comments and general trollishness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

## CONNECTIONS:

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

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





## Facebook uses scanning technologies, alerts authorities about content

By: Cale Guthrie Weissman on 16 July 2012

Posted in Arrests and legal action, Internet tools filtering, Surveillance, United States of America, United States/Canada

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

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

Facebook's software focuses on conversations between members who have a loose relationship on the social network. For example, if two users aren't friends, only recently became friends, have no mutual friends, interact with each other very little, have a significant age difference, and/or are located far from each other, the tool pays particular attention.

The scanning program looks for certain phrases found in previously obtained chat records from criminals, including sexual predators.... The relationship analysis and phrase material have to add up before a Facebook employee actually looks at communications and makes the final decision of whether to ping the authorities.

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

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

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

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

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

### Post new comment

Your name: \*

#### CONNECT WITH ONI

-  [Blog Feed](#)
-  [ONI Newsfeed](#)
-  [@OpenNet](#)
-  [ONI on Facebook](#)

#### OUTSIDE LINKS

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

#### HELP REPORT CENSORSHIP

**HERDICTWEB**

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



E-mail: \*

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

Homepage:

Subject:

Comment: \*

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

CAPTCHA

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

Privacy & Terms

Preview