The Virginian-Pilot

Email searches catch criminals, concern privacy groups

By: Scott Daugherty - January 14, 2013

It started with an email. A message last January from Robert Branson to a Yahoo account.

But an AOL software program flagged a photo he attached as child pornography, and the 46-year-old Chesapeake resident found himself under investigation by police.

Almost a year later, Branson - who faces up to 160 years in prison when he is sentenced later this year - has learned what more and more purveyors of child porn are discovering every year: Email isn't private.

"When it comes to email, you have no reasonable expectation of privacy," said Deputy Public Defender A. Robinson Winn, Branson's attorney.

Thanks to the help of some of the world's largest Internet companies, police and federal agents have pursued and prosecuted thousands of child pornography cases across the country, experts said.

Officials with the National Center for Missing and Exploited Children say they have received 1.7 million tips about child porn since 1998. And while some of those tips were made by concerned citizens who find child porn online, the executive director of the center's Exploited Child Division credits many of them to companies scanning their users' emails, cloud drives and social network sites.

"That is one of the biggest things that is happening," said John Shehan, whose organization was established in 1984 by Congress to serve as a clearinghouse for information about missing children and child pornography. He said the center received more than 400,000 tips in 2012, up from about 326,000 the year before.

Shehan explained that companies such as AOL, Google, Yahoo, Microsoft and Facebook have been legally obligated since 1998 to contact his organization when they find child porn on their network. In the beginning, that meant companies simply alerted the center when one of their customers told them about child porn. Over the past several years, however, many of the companies started using software to actively scour their networks.

"There is a lot of great information coming from these companies... just about everything law enforcement needs to start an investigation," Shehan said. "The apparent child pornography that was sent, the email address they used and the IP address they used."

Privacy advocates are worried about the technology and how Internet companies and the government might choose to use it in the future.

LEGAL ISSUES

The scans are legal because no governmental entity is asking the companies to look at their customers' emails, said Brian J. Gottstein, a spokesman for Virginia Attorney General Ken Cuccinelli.

"These are private companies acting independently of law enforcement to ensure that their private servers are not used to store or traffic contraband," he said. "It is analogous to FedEx or UPS reporting a package they suspect of containing narcotics to authorities."

Julian Sanchez, a research fellow at the Cato Institute, a libertarian think tank based in Washington, said the Electronic Communications Privacy Act is designed to keep companies from releasing their users' private emails. The federal law, however, has an exemption involving child porn and the center. Other instances where companies can release information contained in their customer's private emails: if the communication involves a possible life-threatening emergency or if it involves a crime the company "inadvertently" learned about in the course of its business.

Shehan stressed that no one at the companies is "opening emails and looking inside." It's all automated, he said.

Each company has its own method for scanning its users' emails and online storage drives. But their software programs identify child porn the same way, experts said. The programs analyze a user's photos and videos, assign each image a specific value or digital signature and then compare that signature against a database of known child porn images.

The center's database of digital signatures includes about 18,000 images and videos. Shehan added that some companies have expanded the database to include more photos.

Samantha Doerr, a spokesman for Microsoft's Digital Crimes Unit, said the images in the database are the "worst of the worst." She explained the photos have been verified by law enforcement as child porn.

"These are real crime scene photos," she said.

The database represents just a small fraction of the 80 million photos and videos the center has identified as child porn, but Shehan said "these are the exact types of images law enforcement wants to know about and wants to investigate."

MAKING THE MATCH

Police weren't looking at Branson - who pleaded guilty in September to 11 felonies - until AOL and Yahoo flagged his emails a year ago for containing child porn. According to court documents and testimony, the companies turned the information over to the center, which in turn contacted the Southern Virginia Internet Crimes Against Children Task Force in Bedford County. From there, the Chesapeake Police Department served a search warrant on Branson's mobile home near Indian River.

In all, police found 625 images and 35 videos depicting prepubescent children in sexual situations on Branson's computers, according to Detective Joe Justice of the Chesapeake Police Department. Police also found evidence Branson used email and Skype to send child porn to other people.

While AOL spotted Branson's email, the company's software - and any software that operates like it - can be easily foiled, Microsoft's Doerr said. If a photo is cropped, resized, or otherwise edited, its digital signature changes.

In an effort to find more child porn, Microsoft developed a new software system in 2009 called PhotoDNA. According to Doerr, the software can identify child porn even if the photo has been modified.

"We invest in efforts like this not only because it's the right thing to do, but because we believe there is value to our customers in helping make the Internet a safer place for everyone," said Doerr, noting that Microsoft donated PhotoDNA to the center in 2009 and is now offering it free of charge to any Internet companies interested in using the software.

PhotoDNA - which is now used to scan photos posted on Facebook and Microsoft's SkyDrive, as well as emails sent via Hotmail - works by converting the image to black and white, cropping it to a standard size, carving it into squares and then analyzing each of them separately.

Unlike the software used by AOL and some other companies, PhotoDNA can only analyze photos, not videos.

While law enforcement officials praise the technology as a valuable tool in the fight against child porn, privacy advocates worry about how often PhotoDNA wrongly flags an email as containing child porn.

Giving Microsoft's "best estimates," Doerr said the software returns false positives about once in every two billion images - maybe even less often. She added that some of those false alarms were still child porn; the software flagged a similar photo that was taken shortly before or after the one in the database.

With the volume of images currently posted on the Internet, however, that could mean multiple false alarms per week. More than 144 billion emails were sent each day in 2012, according to The Radicati Group, a technology research firm. Facebook says 300 million new images are uploaded to its site every day.

BIG BROTHER?

Despite the noble intentions behind the scans, privacy advocates say the technology gives companies too much power.

"Child porn is really bad and should be fought, but should you have to fear that you are being watched all the time to prevent its distribution? Because that is what is happening here," said John Whitehead, president of The Rutherford Institute, a civil liberties group based in Charlottesville.

"Every time you turn your computer on, there should be a warning that they are watching you."

In his dissertation, Christopher Soghoian of the ACLU noted that once the technical infrastructure for automatically intercepting and examining a user's communications is in place, AOL or another email provider can easily use it to determine if its customers are "transmitting bomb making instructions, copyrighted images, songs and books, seditious newsletters, or religious texts."

"The impact of this system extends far beyond the company's desire to assist in the discovery of this particularly horrible form of illegal content" wrote Soghoian, a senior policy analyst with the ACLU's Speech, Privacy and Technology Project.

"Such expanded surveillance can be performed, quite easily, if the government provides AOL with a list of additional hashes to add to the company's database and then forces the company to detect the transmission of those other types of prohibited content."

For now, Doerr said Microsoft has no plans to expand the use of PhotoDNA.

"All I know is what it was developed for and what we are using it for, and that is to find child porn," she said.