April 25, 2008 12:25 PM PDT

FBI's Net surveillance proposal raises privacy, legal concerns

Posted by Declan McCullagh | 14 comments

The FBI director and a Republican congressman sketched out a far-reaching plan this we ek for warrantless surveillance of the Internet.

During a House of Representatives Judiciary Committee hearing, the FBI's Robert Mueller and Rep. Darrell Issa of California talked about what amounts to a two-step approach. Step 1 involves asking Internet service providers to open their networks to the FBI voluntarily; step 2 would be a federal law forcing companies to do just that.

Both have their problems, legal and practical, but let's look at step 1 first. Issa su ggested that Internet providers could get "consent from every single person who signed up to operat e under their auspices" for federal police to monitor network traffic for attempts to steal personal information and national secrets. Mueller said "legislation has to be developed" for "some omnibus sea rch capability, utilizing filters that would identify the illegal activity as it comes thr ough and give us the ability to pre-empt" it.

These are remarkable statements. The clearest reading of them points to deep packet inspection of network traffic--akin to the measures Comcast took against BitTorrent and to what Phorm in the United Kingdom has done, in terms of advertising--plus additional processing to detect and thwart any "illegal activity." (See the complete transcript here.)

"That's very troubling," said Greg Nojeim, director of the project on freedom, securit y, and technology at the Center for Democracy and Technology. "It could be an effort to achieve, through unknowing consent, permission to monitor communications in a way that would otherwise be prohibited by law."

Unfortunately, neither Issa nor Mueller recognized that such a plan is probably illega l. California law, for instance, says anyone who "intentionally and without the consent of all parties to a confidential communication" conducts electronic surveillance shall be imprisoned for o ne year. (I say "probably illegal" because their exchange didn't offer much in the way of details.)

"I think there's a substantial problem with what Mueller's proposing," said Al Gidari, a partner at the Perkins Coie law firm who represents telecommunications providers. "He forgets the sta tes have the power to pass more restrictive rules, and 12 of them have. He also forgets that we live in a global world, and the rest of the world doesn't quite see eye to eye on this issue. Th at consent would be of dubious validity in Europe, for instance, where many of our customers resi de."

About The Icono

Declan McCullagh has covere Washington, D.C. for over a d into an iconoclast and a skept oughta have a new federal lav

Subscribe to this
Click this link to view thi

Add this feed to your onlir

The Iconoclast tc

Antitrust

Censorship

Corruption

intellectual property

Latest blog posts from N

Why it's time to dump th for all
Posted in Coop's Corne April 26, 2008 5:00 AM

Digital clothing takes ce

For its part, the FBI isn't talking. After we made repeated attempts to get the bureau to explain what Mueller was talking about, FBI spokesman Paul Bresson responded by saying, "At this point, I'm going to let the director's comments, in the context of the exchange with Rep. Issa, speak for themselves."

What step 1 appears to involve is persuading Internet providers to amend their terms of service and insert an FBI-can-monitor-everything clause. Informed consent is one thing. But does anyone actually read the fine print on their contracts with their broadband or wireless provider? If not, is that fine print good enough?

Informed consent is important because of the wording of the Electronic Communications Privacy Act, or ECPA, which says providers may share the contents of customers' communications only "with the lawful consent" of the user. Otherwise, providers are breaking the law and can be sued for damages. And without consent, the FBI would bump up against the Fourth Amendment's prohibition on unreasonable searches.

Originally, Congress seemed to take a liberal view of what constituted "lawful consent." When ECPA was enacted in 1986, a House committee report said "consent may be inferred from a course of dealing," and if "those rules are available to users," consent can be implied.

But that was written way back in the early, pre-Internet days of Compuserve and bulletin board systems. More recently, courts have interpreted ECPA more strictly.

The 2003 In Re Pharmatrak decision from the U.S. Court of Appeals for the 1st Circuit offers one useful measuring stick. The court ruled in a case involving Web tracking "that it makes more sense to place the burden of showing consent on the party seeking the benefit of the exception." The judges approvingly cited a second case, which said "consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception."

The Federal Trade Commission, too, has taken a relatively strict view of informed consent. In its lawsuit filed against Odysseus Marketing, the FTC argued that it was unlawful for a company not "to adequately disclose" to customers that it was sharing information with third parties. The case ended in a settlement.

Translation: Obtaining "lawful consent" for FBI monitoring means making sure that your customers actually know what's going on and agree. Hiding it in the terms of service doesn't qualify.

But assume that the FBI can persuade Internet providers to include a prominent notice in every monthly bill, or some other mechanism that would be legally sufficient. Another problem is that even if the person who pays the bills consents to monitoring, other people may use the connection--think homes with open wireless connections. ECPA's legal protections follow individual people, not customer accounts.

Rewriting U.S. surveillance laws

Because the FBI would run into serious problems doing wide-scale Internet surveillance under existing state and federal law, step 2 may be necessary. That means rewriting U.S. surveillance law.

Issa said he wants to "craft" legislation that would give the FBI the power to look "for those illegal activities, and then act on those, both defensively and, either yourselves or certainly other agencies, offensively in order to shut down a crime in process." He worried about "national-security secrets and just the common information of private individuals" being at risk. In his response, Mueller said he wants Congress to "give us the ability to pre-empt that illegal activity."

"Looking for" a crime in process on the Internet can take multiple paths. If it's a denial-of-service


Exploratorium
Posted in Geek Gestalt
April 25, 2008 10:40 P


Report: Google unworrie
antitrust issue
Posted in News Blog by
April 25, 2008 5:12 PM


New iPhone back in bla
Posted in One More Thi
April 25, 2008 4:14 PM


More Google Docs avai
presentations
Posted in News Blog by
April 25, 2008 3:45 PM

Featured blogs

Beyond Binary by Ina Frie
A look at how technology is
people behind all that life-cha

Coop's Corner by Charles
Charles Cooper weighs in or
doesn't suffer fools gladly.

Defense in Depth by Robe
Covering the latest in compu
crime.

Geek Gestalt by Daniel Te
At the tech culture nexus of
virtual worlds.

Green Tech
Fresh green tech news and

One More Thing by Tom K
Tom Krazit takes on the tech
and keeps a close watch on

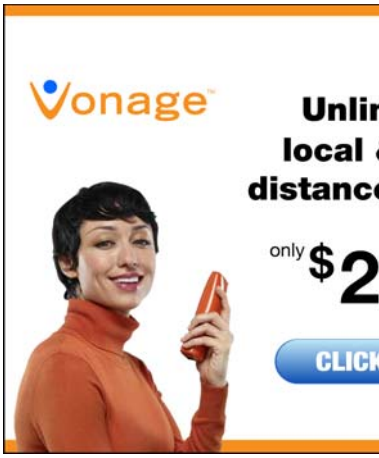
Outside the Lines by Dan
When business and technolo
get interesting.

The Social by Caroline Mc
Exploring all facets of social

Underexposed by Stephe
Coverage of digital photogra
open-source software.

More CNET blogs »

Ad Fe



"national-security secrets," as well as personal information being transferred, deep packet inspection would be necessary--roughly on a scale of the Great Firewall of China.

Needless to say, detecting "illegal activity" would soon be extended to copyright infringement and peer-to-peer networks. Under the No Electronic Theft Act, swapping music or video files is a federal crime, if the total value of the files exceeds $1,000. If the value tops $2,500, the penalties jump up to not more than five years in prison. And as Jammie Thomas found out last year, allegedly sharing 24 files can lead to $222,000 in civil penalties.

"I think you bump squarely into the Fourth Amendment when you get into the required waiver of constitutional protections to use a service," said Gidari, the attorney at Perkins Coie. "Why don't we extend it to include not criticizing the government? Which right is next? 'You may use our service, as long as you don't disparage Verizon?' Why not that one?...You've still got to have, at the end of the day, a constitutionally supportable legal process to get access to anyone's communications. This cannot be an end run around that."

The problem of how to "shut down a crime in process" and "pre-empt that illegal activity" is more difficult and, perhaps, more worrisome.

Here's what Kurt Opsahl, a senior staff attorney at the Electronic Frontier Foundation in San Francisco, had to say when I asked him to read the transcript of Wednesday's hearing:

> It certainly is Mueller's responsibility to explain what it is that he's looking for. But it seems that he's saying, essentially, that the surveillance society is the best society. A society in which the government has complete information about illegal activities and is able to enforce that. Throughout our country's existence, we've lived in a society where the government doesn't have perfect information.
>
> Is (Mueller) suggesting that there's a search capability using filters that would identify an infringing work and fail to deliver a message containing that work? Is that the choke point? If that is the case, how can that be done well? How about fair uses? How will the government tell whether a copyrighted work is sent pursuant to a license? Will it have a centralized database of licenses? How does he propose to have this work, so it only identifies illegal activities and doesn't overly choke?
>
> The FBI has some obligation to explain: what is it going to focus on here? Once you have the technology in place, will it then be used for more and more?

If you thought the tussles over Net neutrality were heated before, imagine a broadband provider throttling certain applications--and being able to blame that throttling capability on law enforcement. At the very least, it would be a wonderful excuse.

Which is why it's a shame, and somewhat troubling, that the FBI has chosen not to say what its director is proposing (and apparently will be working with Congress to write into law).

Odds of FBI-filtering legislation: Zero?

One possible germ for this Internet-monitoring idea lies in Homeland Security's so-called Einstein program, which is designed to monitor Internet mischief and network disruptions aimed at federal agencies. Not much about Einstein is public, but a privacy impact assessment offers some details.

Homeland Security Spokeswoman Laura Keehner said in a telephone interview that the primary focus of Einstein at the moment is protecting federal-government networks. "Obviously, the FBI could clarify or elaborate on what they said," Keehner said. "I do know that (from Homeland

Security's perspective) we now first need to get our .gov in order. We need to concentrate on our federal networks...We're also bringing in the private sector to open those lines of discussion and figure out ways that the private sector can better equip themselves to stop any cyberincursions."

Another possibly related effort is the Bush administration's so-called Cyber Initiative. In January, President Bush signed a pair of secret orders--National Security Presidential Directive 54/Homeland Security Presidential Directive 23--that apparently deal with detecting and preventing Internet disruptions. Issa is a member of the House Intelligence Committee, which held a closed-door hearing
on Thursday devoted to the Cyber Initiative--and, during the exchange with Mueller a day earlier, he said his monitoring idea was related.

The House Intelligence committee didn't want to talk. But a representative of the House Homeland Security committee chaired by Rep. Bennie Thompson (D-Miss.) sent us three bullet points in an e-mail message:

> 1. Chance of a legislative initiative that would allow FBI to place filters to identify illegal activity at choke points on the .com space: 0
>
> 2. We still have concerns and questions about the initiative, and we continue to do oversight.
>
> 3. Legislation is not being considered for any of the new proposals, outside of the budget requests made by the administration.

Point No. 3 seems to relate to the administration's 2009 budget request, which asks Congress for $293.5 million to expand Einstein to the entire federal government.

The Senate Homeland Security and Governmental Affairs Committee, which is headed by Joe Lieberman of Connecticut, also held a classified hearing last month on the administration's Cyber Initiative.

But a committee aide told us, "The idea of filtering for criminal activity has never been discussed with us. Nor has any new statutory authority been discussed. In fact, the administration explicitly said it didn't need any legislation. Furthermore, the idea of monitoring nongovernment domains has never been proposed in briefings the committee has received."

It's true that, at least in the current political climate, legislation of the sort Issa wants to draft isn't likely to slide through Congress unopposed.

Still, it's worth keeping in mind that the FBI has a recent, and not very flattering, history of trying to expand the scope of surveillance methods. Bureau agents used so-called exigent letters to obtain records from telephone companies, claiming that an emergency situation existed.

In reality, there was often no emergency at all. The Justice Department's inspector general found similar abuses of national-security letters. The FBI also tried to bypass the Foreign Intelligence Surveillance Court when it denied requests to obtain records.

Perhaps Mueller can provide a convincing argument for why laws giving the FBI "omnibus search capability utilizing filters that would identify the illegal activity" would be wise. Perhaps not. But when politicians weigh the idea of trusting the FBI with such broad and unprecedented authority, they should consider the abuses that have already taken place with far less powerful tools.

CNET News.com's Anne Broache contributed to this report.

TOPICS: Privacy

TAGS: FBI, Robert Mueller, surveillance, Net neutrality **BOOKMARK:** Digg Del.icio.us Reddit

Recent posts from The Iconoclast

FBI's Net surveillance proposal raises privacy, legal concerns

Transcript: FBI director on surveillance of 'illegal' Internet activity

FBI, politicos renew push for ISP data retention laws

Shamos: Why e-voting paper trails are a bad idea

FBI nudges state 'fusion centers' into the shadows

TalkBack

14 comments
Post a comment

Publishing
epcraig
Apr 25, 2008, 10:15 PM PDT

Famous words
b4igo2gat
Apr 25, 2008, 6:19 PM PDT

What has happened to this country?
sam99999999
Apr 25, 2008, 4:08 PM PDT

FBI's surveillance
b4igo2gat
Apr 25, 2008, 2:32 PM PDT

I got an idea.
Imalittleteapot
Apr 25, 2008, 2:31 PM PDT

This sucks.
jessiethe3rd
Apr 25, 2008, 2:23 PM PDT

Read more comments >