CRYPTOWARS, THE OBFUSCATION

The US Courts released its semiannual Wiretap Report the other day, which reported that very few of the attempted wiretaps last year were encrypted, with even fewer thwarting law enforcement.

> The number of state wiretaps in which encryption was encountered decreased from 41 in 2013 to 22 in 2014. In two of these wiretaps, officials were unable to decipher the plain text of the messages. Three federal wiretaps were reported as being encrypted in 2014, of which two could not be decrypted. Encryption was also reported for five federal wiretaps that were conducted during previous years, but reported to the AO for the first time in 2014. Officials were able to decipher the plain text of the communications in four of the five intercepts.

Motherboard has taken this data and concluded it means the Feds have been overstating their claim they're "going dark."

> [N]ew numbers released by the US government seem to contradict this doomsday scenario.
>
> [snip]
>
> "They're blowing it out of proportion," Hanni Fahkoury, an attorney at the digital rights group Electronic Frontier Foundation (EFF), told Motherboard. "[Encryption] was only a problem in five cases of the more than 3,500 wiretaps they had up. Second, the presence of encryption was down by almost 50 percent from the previous year.
>
> "So this is on a downward trend, not

> upward," he wrote in an email.

Much as I'd like to, I'm not sure I agree with Motherboard's (or Hanni Fahkoury's) conclusion.

Here's what the data show since 2012, which was the first year jurisdictions reported being unable to break encryption (2012; 2013):

Year	Total Fed	Total Encrypted	%	Total Fed Unbroken	%	Total State	Total Encrypted	%	Total State Unbroken	%
2012	1354	NR	NR	NR	NR	2041	15 (+52) (+7)	.73%	4	.19%
2013	1476	NR	NR	NR	NR	2100	41	1.9%	9	.42%
2014	1279	(5)	NR	(1)	NR	2275	22	.96%	2	.08%

You'll see lots of parenthetical entries and NRs. That's because this data is not being reported systematically. Parenthetical references are to encrypted feeds not reported until years after they get set, and usually those have been decrypted by the time they're reported. NRs show that we have not getting these numbers, if they exist, from federal law enforcement (and the numbers *can't* be zero, as reported here, because FBI has been taking down targets like Silk Road). The reporting on this ought to raise real questions about the quality of the data being reported and perhaps might spark some interest in mandating better reporting of this data so it can be tracked. But it also suggests that — at a time when law enforcement are just beginning to find encryption they can't break (immediately) — there's a lot of noise in the data. Does 2013's 2% of encrypted targets and half-percent that couldn't be broken represent a big problem? It depends on who the target is — a point I'll come back to.

Congress will soon have that opportunity (but won't avail themselves of it).

Even as US Courts were reporting still very low levels of encryption challenges faced by law enforcement, both the Senate Judiciary Committee and the Senate Intelligence Committee announced hearings next Wednesday where Jim Comey will have yet another opportunity to try to present a compelling argument that he should have back

doors into our communication. SJC even saw fit to invite witnesses with opposing viewpoints, which the "intelligence" committee saw no need to do.

In an apparent attempt to regain some credibility before these hearings (Jim Comey is nothing if not superb at working the media), Comey went to Ben Wittes to suggest his claimed concern with increasing use of encryption has to do with ISIS' increasing use of encryption. Ben quotes from Comey's earlier comments to CNN then riffs on that in light of what Comey just told him in a conversation.

> > "Our job is to find needles in a nationwide haystack, needles that are increasingly invisible to us because of end-to-end encryption," Comey said. "This is the 'going dark' problem in high definition."
>
> > Comey said ISIS is increasingly communicating with Americans via mobile apps that are difficult for the FBI to decrypt. He also explained that he had to balance the desire to intercept the communication with broader privacy concerns.
>
> > "It is a really, really hard problem, but the collision that's going on between important privacy concerns and public safety is significant enough that we have to figure out a way to solve it," Comey said.
>
> Let's unpack this.
>
> As has been widely reported, the FBI has been busy recently dealing with ISIS threats. There have been a bunch of arrests, both because ISIS has gotten extremely good at the inducing self-

> radicalization in disaffected souls worldwide using Twitter and because of the convergence of Ramadan and the run-up to the July 4 holiday.
>
> As has also been widely reported, the FBI is concerned about the effect of end-to-end encryption on its ability to conduct counterterrorism operations and other law enforcement functions. The concern is two-fold: It's about data at rest on devices, data that is now being encrypted in a fashion that can't easily be cracked when those devices are lawfully seized. And it's also about data in transit *between* devices, data encrypted such that when captured with a lawful court-ordered wiretap, the signal intercepted is undecipherable.
>
> [snip]
>
> What was not clear to me until today, however, was the extent to which the ISIS concerns and the "going dark" concerns have converged. In his Brookings speech, Comey did not focus on counterterrorism in the examples he gave of the going dark problem. In the remarks quoted by CNN, and in his conversation with me today, however, he made clear that the landscape is changing fast. Initial recruitment may take place on Twitter, but the promising ISIS candidate quickly gets moved onto messaging platforms that are encrypted end to end. As a practical matter, that means there are people in the United States whom authorities reasonably believe to be in contact with ISIS for whom surveillance is lawful and appropriate but for whom useful signals interception is not technically feasible.

Now, Ben incorrectly blurs the several roles of FBI here. FBI's interception of ISIS communiques

may be *both* intelligence and law enforcement. To the extent they're the former — to the extent they're conducted under FISA — they won't show up in US Courts' annual report.

But they probably should, if Comey is to have any credibility on this front.

Moreover, Ben simply states that "there are people in the United States whom authorities reasonably believe to be in contact with ISIS for whom surveillance is lawful and appropriate." But there's no evidence presented to support this. Indeed, most of the so-called ISIS prosecutions have shown 1) where probable cause existed, it largely existed in the clear, in Twitter conversations and other online postings and 2) there may not have been probable cause before FBI ginned it up.

It ought to raise real questions about whether Comey's going dark problem is a law enforcement one — with FBI being unable to to access evidence on real criminals — or is an intelligence one — with FBI being unable to access First Amendment protected speech that nevertheless may be important for an understanding of the threat ISIS poses domestically. Again, the data is not there, one way or another, but given the law enforcement data, we ought to demand real numbers for intelligence intercepts. Another pertinent question is whether this encrypted data is easily accessible to NSA (ISIS recruiters are almost entirely going to be legitimate NSA targets located overseas), but not to FBI?

And all this presumes that Comey is telling the truth about ISIS and not — as he and just about every member of the Intelligence Community has done routinely — used terror threats to be able to get authorities to wield against other kinds of threats, especially hackers (which is not to say hackers aren't a target, just that the IC likes to pretend its authorities serve an exclusively CT purpose when they clearly do not). The law enforcement data, at least, show that even members of very sophisticated drug

distribution networks are using encryption at a really low level. Is ISIS' ability to coach potential recruits into using encrypted products on Twitter really that much better, or is Comey really talking about hackers who more obviously have the technical skills to encrypt their communications?

Thus far, Comey would have you believe that intelligence — counterterrorism — targets encrypt at a much higher rate than even drug targets. But the data also suggest even federal law enforcement (that is, Comey's agency, among others) aren't tracking this very effectively, and so can't present reliable numbers.

Before we go any further in this cryptowar debate, we ought to be able to get real numbers on how serious the problem is.