FBI NOW CLAIMING SECTION 215 (WHICH IS DIFFERENT THAN THE PHONE DRAGNET) HAS A BIG ROLE IN HACKING INVESTIGATIONS

Admittedly, after its alarmism on encryption, one should always treat FBI claims about necessary tools skeptically. But I'm interested in the claim, made by FBI's Assistant Director of its Cyber Division, that the Bureau relies on 215 for computer intrusion investigations.

> The FBI's cyber crime investigations would "obviously" suffer if Congress doesn't reauthorize Section 215 of the Patriot Act, which allows the FBI to request business records from major companies.
>
> "If that expires, obviously it's going to impact what we do as an organization and certainly on cyber," said Joseph Demarest, assistant director of the FBI's Cyber Division, during a roundtable discussion with reporters Tuesday.
>
> Congress must reauthorize the controversial portion of the law by June 1. Civil liberties advocates argue the 215 program is an invasion of privacy, granting the National Security Agency (NSA) blanket authority to spy on Americans.
> But two leaders of the FBI's digital crime unit said losing the program would reduce the bureau's effectiveness.
>
> The business records request program based on Section 215 allows the FBI to obtain customer records from places like

> major telecom companies without going through the public court system.
>
> "We use that in working with, I'll say major providers," Demarest said. "And we're looking at historical records."
>
> "Not having the ability to use that as a vehicle to obtain that information," Demarest added, "that's the problem we face."
>
> The FBI argues that the 215 program approach allows investigators to go after cyber crooks without tipping their hand to possible accomplices.

Let me interject and note that the reporting on this — and therefore presumably the questions asked at this little eat-the-journalists-for-lunch-event — was atrocious.

The guy in charge of hacking told a group of reporters they rely on Section 215 to investigate hacking. And several of those reporters then reported that he said they needed the phone dragnet.

If true, that would be huge news, because the phone dragnet has pretty tight controls limiting its use to terrorists and Iran. So if the NSA is now also using the phone dragnet to catch hackers, it means the government has blown up the definition of hackers even further than they obviously have.

But it's unlikely that's what Demarest meant, though that doesn't mean his comment, if true, isn't newsworthy for other reasons.

The reporters claiming the FBI uses the phone dragnet to catch hackers are — as far too many activist organizations do — probably conflating the phone dragnet, a program authorized by Section 215, with Section 215, which authorizes the collection of a lot more things — things like money transfers, explosives precursors, hotel records, probably credit card data, and Internet records — including in what you and I

would call bulk, even if Bob Litt would not.

There were roughly 180 Section 215 orders last year. Only 5 of those orders supported the phone dragnet.

I'm guessing, but probably what Demarest was talking about is FBI's (note, not NSA's) reliance, since 2009, to collect records from Internet companies. At least during 2011 and 2012, the majority of the Section 215 orders were for Internet records.

We can say a few things about this collection. First, FBI conducted the collection using NSLs until 2009, when publication of an OLC opinion limiting the interpretation of phone records covered by NSLs led the Internet companies to successfully challenge the use of NSLs to collect that data anymore. This collection obtains "electronic communication transaction records," but for something other than the Internet equivalent of call time and participants (because that's what the OLC opinion excluded). These orders are probably fairly programmatic, because it can take 30 to 40 days to obtain a Section 215 order (meaning the FBI would run whatever collection on a set of standing orders, just like they do the phone dragnet). And these collections are probably substantive enough that FISC imposed minimization procedures on the collection.

And, we can now guess (assuming, of course, the FBI isn't talking out of its arse again) that these collections support cyberinvestigations.

One reason this is important, however, is that it changes the stakes for reauthorization of Section 215. If the FBI considers this mission critical, it means activists should account for this collection when they consider the leverage they have in debates moving forward.