

# RON WYDEN HINTS AT HOW THE INTELLIGENCE COMMUNITY HIDES ITS WEB TRACKING UNDER SECTION 215

Ron Wyden had an amendment to Section 215 that would have limited the use of that provision to obtain web traffic information that fell one vote short in the Senate, partly because Nancy Pelosi whipped Tom Carper against it and partly because two Senators (Bernie Sanders and Patty Murray) didn't get back for a vote. In an effort to resuscitate the amendment in the House under Zoe Lofgren and Warren Davidson's leadership (which would surely pass if Section 215 got bounced back to the Senate), Ron Wyden released a letter to Ric Grenell trying to force some transparency about how the IC hides the scope of the use of Section 215 to get web search and Internet traffic information.

The letter asks Grenell to explain how Section 215 orders served on IP addresses, rather than email addresses, might get counted in transparency provisions.

How would the government apply the public reporting requirements for Section 215 to web browsing and internet searches? In this context, would the target or "unique identifier" be an IP address?

If the target or "unique identifier" is an IP address, would the government differentiate among multiple individuals using the same IP address, such as family members and roommates using the same Wi-Fi network, or could numerous users appear as a single target or "unique identifier"?

If the government were to collect web

browsing information about everyone who visited a particular website, would those visitors be considered targets or “unique identifiers” for purposes of the public reporting? Would the public reporting data capture every internet user whose access to that website was collected by the government?

If the government were to collect web browsing and internet searches associated with a single user, would the public reporting requirement capture the scope of the collection? In other words, how would the public reporting requirement distinguish between the government collecting information about a single visit to a website or a single search by one person and a month or a year of a person’s internet use?

Wyden here lays out three use cases for how the IC might (one should assume does) use Section 215 to get web traffic.

- An order in which an IP address used by multiple people is the target
- An order collecting all the people who visit a particular website
- An order collecting all the web browsing and internet searches of a single user

The government is required to report:

(5) the total number of orders issued pursuant to applications made under section 1861(b)(2)(B) of this title and a good faith estimate of—

(A) the number of targets of such orders; and

(B) the number of unique identifiers used

to communicate information collected pursuant to such orders;

Taking each of his three scenarios, here's what I believe the government would report.

## **An order in which an IP address used by multiple people is the target**

In the first scenario, the government is trying to obtain everyone who "uses" a particular IP address. The scenario laid out by Wyden is a WiFi router used by family or friends, but both because the House Report prohibited such things in 2015 and because DOJ IG has raised questions about targeting everyone who uses a Friends and Family plan, I doubt that's what the IC really does.

Rather, I suspect this is about VPNs and other servers that facilitate operational security. The government could hypothetically obtain four orders a year getting "VPNs," requiring providers of each of the 10 major VPNs in the country to provide the IP addresses of all the incoming traffic, which would show the IP addresses of everyone who was using their location obscuring traffic.

In such a case, the targeted VPN IP addresses wouldn't be communicating information at all. The users would get no information back. Therefore, the IC would only report the number of targets of such orders. If the "target" were defined as VPN, the number would be reported as 4 (for each of the 4 orders); if the "target" were defined as the specific VPN providers, the number of targets would be reported as 10.

The IC would entirely hide the number of individual Americans affected.

## **An order collecting all the people who visit a particular website**

This application would seek to learn who visited a particular website. The classic case would be *Inspire* magazine, the AQAP propaganda. But I could also see how the IC might want to collect people who visit WikiLeaks' submission page, or any number of sites that would offer information of interest to foreign spies (even DNI's report on surveillance collection!). In such a use case, the government might ask not for the information provided to the user, but instead the incoming IP addresses of every request to the website. Again, this would not reflect a communication of information (and certainly not to the end user), so would not be reported under 5B.

If the targets were defined as "AQAP propaganda sites," *Inspire* and all its affiliates might be reported as just one target (or might even be counted on a more generalized 215 order targeting AQAP or WikiLeaks, and so not as a unique 215 order at all).

The end users here would, again, not be counted if the collection request deliberately asked for something that did not "communicate information," though I'm not sure precisely what technical language the government would use to accomplish this.

## **An order collecting all the web browsing and internet searches of a single user**

This use case would ask how a 215 order targeting an individualized target (like Carter Page) shows up in transparency reports. If this were an order served on Google targeting a

single account identifier for Google (say, Page's Gmail account), the government might treat that Gmail identifier as the unique identifier, even though the government was getting information on every time this unique identifier obtained information.

Even in the criminal context, prosecutors don't always target Google histories (for example, they did not with Joshua Schulte, and so got Google searches going back to before he joined the CIA). In the intelligence context, the FBI is given even more leeway to obtain everything, based off the logic that it's harder to find clandestine activity.

In other words, Wyden has pointed to three use cases, all of which the IC is surely using, which existing transparency reporting requirements would entirely obscure the impact of.