

SECTION 702 USED FOR CYBERSECURITY: YOU READ IT HERE FIRST

I have been reporting for years that the government uses Section 702 for cybersecurity purposes, including its upstream application.

- June 10, 2013: Hacking was the biggest success story for 702
- August 7, 2013: Me, saying I told you so
- October 21, 2013: An upstream application of 702 to cyber was NSA's big 702 success story
- November 7, 2013: The original (good) version of USA Freedom Act would have given NSA 6 months to shut down upstream 702 targeting for cyber
- November 23, 2013: NSA denies their admitted use of 702 for cyber targets
- July 3, 2014: PCL0B hides the use of 702 for cyber targets
- February 4, 2015: Cyberattacks are one of the crimes FBI can use 702 data to prosecute
- February 10, 2015: How Jeffrey White misused PCL0B to dismiss the possibility of domestic wiretapping

under upstream in EFF-related suits

ProPublica and NYT have now confirmed and finally liberated related Snowden documents on the practice. They show that DOJ tried to formalize the process in 2012 (though I have reasons to doubt that the NSA documents released tell all of the story, as I hope to show in upcoming posts).

Without public notice or debate, the Obama administration has expanded the National Security Agency's warrantless surveillance of Americans' international Internet traffic to search for evidence of malicious computer hacking, according to classified NSA documents.

In mid-2012, Justice Department lawyers wrote two secret memos permitting the spy agency to begin hunting on Internet cables, without a warrant and on American soil, for data linked to computer intrusions originating abroad – including traffic that flows to suspicious Internet addresses or contains malware, the documents show.

The Justice Department allowed the agency to monitor only addresses and “cybersignatures” – patterns associated with computer intrusions – that it could tie to foreign governments. But the documents also note that the NSA sought to target hackers even when it could not establish any links to foreign powers.

The disclosures, based on documents provided by Edward J. Snowden, the former NSA contractor, and shared with the New York Times and ProPublica, come at a time of unprecedented cyberattacks on American financial institutions, businesses and government agencies, but also of greater scrutiny of secret legal justifications for broader government surveillance.

Jonathan Mayer, whom ProPublica and NYT cite in the article, has his own worthwhile take on what the documents say.

Stay tuned!