JACK GOLDSMITH'S CODE

On May 6, 2004, Jack Goldsmith signed an OLC memo that read, in part,

> We conclude that in the circumstances of the current armed conflict with al Qaeda, the restrictions set out in FISA, as applied to targeted efforts to intercept the communications of the enemy in order to prevent further armed attacks on the United States, would be an unconstitutional infringement on the constitutionally assigned powers of the President. The President has inherent constitutional authority as Commander in Chief and sole organ for the nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States. Congress does not have the power to restrict the President's exercise of that authority.
>
> [snip]
>
> Finally, as part of the balancing of interests to evaluate the Fourth Amendment reasonableness, we think it is significant that [redacted] is limited solely to those international communications for which "there are reasonable grounds to believe … [that] a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group." March 11, 2004 Authorization [redacted] The interception is thus targeted precisely at communications for which there is already a reasonable basis to think there is a terrorism connection. This is relevant because the Supreme Court has indicated that in evaluating

> reasonableness, one should consider the "efficacy of [the] means for addressing the problem."
>
> [snip]
>
> Thus, a program of surveillance that operated by listening to the content of every telephone call in the United States in order to find those calls that might relate to terrorism would require us to consider a rather difference [sic] balance here. [redacted] however, is precisely targeted to intercept solely those international communications for which there are reasonable grounds already to believe there is a terrorism connection, a limitation which further strongly supports the reasonableness of the searches.

We now know that opinion not only authorized the wiretapping of calls involving US persons, but also at least assumed the collection and contact chaining of the call records of all Americans (there's an almost entirely redacted section of the memo that describes the March 19 halt to the collection of Internet metadata and the April 2 modification we don't yet know about).

It's worth keeping in mind that Goldsmith laid out the case that such a program was "reasonable" under the Fourth Amendment as you read his current writing on the NSA. For example, when — several weeks ago — he scolded the White House for not more aggressively defending the program that has actually expanded since he authorized it 9 years ago…

> The government cannot rely on outsiders to explain these documents. It must do so itself, aggressively and comprehensively, even at the expense of revealing more classified information or having to acknowledge embarrassing information. If it doesn't do so, the information already leaked, and the

> information that will be leaked in the weeks and months ahead, will continue to be portrayed in a very unfavorable light.

He was in part calling for the White House to protect programs he — back in 2004 — deemed critical to protect against terrorism.

Even more interesting is Goldsmith's prediction (funded by Northrop Grumman, which is a significant NSA contractor) that we'll all learn to welcome NSA scanning all the metadata and content of US communications — searches far more intrusive, and not committed under the guise of war — in search of hackers in the future.

> "I can't defend the country until I'm into all the networks," General Alexander reportedly told senior government officials a few months ago.
>
> For Alexander, being in the network means having government computers scan the content and metadata of Internet communications in the United States and store some of these communications for extended periods. Such access, he thinks, will give the government a fighting chance to find the needle of known malware in the haystack of communications so that it can block or degrade the attack or exploitation. It will also allow it to discern patterns of malicious activity in the swarm of communications, even when it doesn't possess the malware's signature. And it will better enable the government to trace back an attack's trajectory so that it can discover the identity and geographical origin of the threat.
>
> Alexander's domestic cybersecurity plans look like pumped-up versions of the NSA's counterterrorism-related homeland surveillance that has sparked so much

> controversy in recent months. That is why so many people in Washington think that Alexander's vision has "virtually no chance of moving forward," as the Times recently reported. "Whatever trust was there is now gone," a senior intelligence official told Times.
>
> There are two reasons to think that these predictions are wrong and that the government, with extensive assistance from the NSA, will one day intimately monitor private networks.
>
> The first is that the cybersecurity threat is more pervasive and severe than the terrorism threat and is somewhat easier to see. If the Times' website goes down a few more times and for longer periods, and if the next penetration of its computer systems causes large intellectual property losses or a compromise in its reporting, even the editorial page would rethink the proper balance of privacy and security. The point generalizes: As cyber-theft and cyber-attacks continue to spread (and they will), and especially when they result in a catastrophic disaster (like a banking compromise that destroys market confidence, or a successful attack on an electrical grid), the public will demand government action to remedy the problem and will adjust its tolerance for intrusive government measures. [my emphasis]

Even under the expansive interpretation of that May 2004 memo, it would take a remarkable argument to claim such searches could be "reasonable" under the Fourth Amendment, though Goldsmith did just that in a Brookings paper in 2010.

But there's something else.

Goldsmith may be right that if an entire region loses power thanks to a hack they'll embrace the dragnet (though some people attribute the 2003 Northeast outage to just such a hack or at least to a virus, and it hasn't generated support for such surveillance yet).

But part of the process for developing such support, he argues, is continued "transparency" from the NSA.

Yet Goldsmith doesn't mention — and with this one exception, no one at Lawfare appears to have — the allegations that the NSA has worked to weaken encryption standards. And even if you doubt that NYT report (though Bruce Schneier has seen related documents and he still seems to believe it), no one doubts that the NSA purchases exploits and uses them, rather than alerting the targets of the flaw.

Thus, it's no longer so simple as extending "special needs" yet further, as Goldsmith does, to keep the nation safe. Because, even if you applaud NSA's intelligence collection programs (that rely on weakening encryption and, to conduct the kind of massive scanning envisioned, would require breaking Tor), the NSA is now a significant part of the problem.

Schneier lays this out in an essay defending the publication of details on NSA's hacking.

> The NSA not only develops and purchases vulnerabilities, but deliberately creates them through secret vendor agreements. These actions go against everything we know about improving security on the Internet.
>
> It's folly to believe that any NSA hacking technique will remain secret for very long.
>
> [snip]
>
> It's equal folly to believe that the NSA's secretly installed backdoors will remain secret. Given how inept the NSA

> was at protecting its own secrets, it's extremely unlikely that Edward Snowden was the first sysadmin contractor to walk out the door with a boatload of them. And the previous leakers could have easily been working for a foreign government. But it wouldn't take a rogue NSA employee; researchers or hackers could discover any of these backdoors on their own.
>
> [snip]
>
> The NSA has two conflicting missions. Its eavesdropping mission has been getting all the headlines, but it also has a mission to protect US military and critical infrastructure communications from foreign attack. Historically, these two missions have not come into conflict. During the cold war, for example, we would defend our systems and attack Soviet systems.
>
> But with the rise of mass-market computing and the Internet, the two missions have become interwoven. It becomes increasingly difficult to attack their systems and defend our systems, because everything is using the same systems: Microsoft Windows, Cisco routers, HTML, TCP/IP, iPhones, Intel chips, and so on. Finding a vulnerability — or creating one — and keeping it secret to attack the bad guys necessarily leaves the good guys more vulnerable.
>
> Far better would be for the NSA to take those vulnerabilities back to the vendors to patch. Yes, it would make it harder to eavesdrop on the bad guys, but it would make everyone on the Internet safer. If we believe in protecting our critical infrastructure from foreign attack, if we believe in protecting Internet users from repressive regimes worldwide, and if we believe in

> defending businesses and ourselves from cybercrime, then doing otherwise is lunacy.
>
> It is important that we make the NSA's actions public in sufficient detail for the vulnerabilities to be fixed. It's the only way to force change and improve security.

This is far more transparency than the NSA has embraced — or than Goldsmith, even (and he has at least noted the NSA's hypocrisy when it wails about China's hacking of us).

Something more than a Congressionally authorized (or secret OLC rubber stamp) expansion of special needs is needed, and really should be backed by anyone claiming cyberattacks pose this dire a threat. Because right now the NSA is making us less safe, all in the name of national security.