Snowden disclosures finally hit 12 on a scale of 1 to 10

motherjones.com

A few days ago, NBC News quoted a former intelligence official about the fallout from Edward Snowden's NSA leaks. "The damage, on a scale of 1 to 10, is a 12," he said.

At the time, I thought it was an odd thing to say. Obviously Snowden's leaks have been damaging to the NSA, and just as obviously they've caused the NSA enormous PR problems. Still, we've known for years that they were collecting telephone metadata. We've known they were subpoenaing email and online documents from tech providers like Google and Microsoft. We've known they were monitoring switching equipment and fiber optic cables. We certainly know a lot more *details* about this stuff than we used to, but the basic outline of NSA's capabilities hasn't really come as much of a surprise.

So what was this former intelligence official talking about? I suspect it was this:

> **The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems,** protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.
>
> ....Some of the agency's most intensive efforts have focused on the encryption in universal use in the United States, including Secure Sockets Layer, or SSL; virtual private networks, or VPNs; and the protection used on fourth-generation, or 4G, smartphones.
>
> ....By this year, the Sigint Enabling Project had found ways inside some of the encryption chips that scramble information for businesses and governments, either by working with chipmakers to insert back doors or by exploiting security flaws, according to the documents. The agency also expected to gain full unencrypted access to an unnamed major Internet phone call and text service; to a Middle Eastern Internet service; and to the communications of three foreign governments.
>
> ....[In 2010, a] briefing document claims that the agency had developed **"groundbreaking capabilities"** against encrypted Web chats and phone calls. Its successes against Secure Sockets Layer and virtual private networks were gaining momentum.
>
> But the agency was concerned that it could lose the advantage it had worked so long to gain, if the mere "fact of" decryption became widely known. **"These capabilities are among the Sigint community's most fragile, and the inadvertent**

> **disclosure of the simple ‘fact of’ could alert the adversary and result in immediate loss of the capability,”** a GCHQ document warned.

That's a 12 on a scale of 1 to 10. The Snowden documents don't make clear precisely what NSA's capabilities are, or exactly what kind of encryption it can break. Nor is it clear how many of its new capabilities are truly due to mathematical breakthroughs of some kind, and how many are more prosaic hacking exploits that have given them more encryption keys than in the past.

Nonetheless, this is truly information that plenty of bad guys probably didn't know, and probably didn't have much of an inkling about. It's likely that many or most of them figured that ordinary commercial crypto provided sufficient protection, which in turn meant that it wasn't worth the trouble to implement strong crypto, which is a bit of a pain in the ass. (Recall, for example, Glenn Greenwald's admission that he "almost lost one of the biggest leaks in national-security history" because Snowden initially insisted on communicating with strong crypto and Greenwald didn't want to be bothered to install it.)

But now that's all changed. Now every bad guy in the world knows for a fact that commercial crypto won't help them, and the ones with even modest smarts will switch to strong crypto techniques that remain unbreakable. It's still a pain in the ass, but it's not that big a pain in the ass.

For what it's worth, this is about the point where I get off the Snowden train. It's true that some of these disclosures are of clear public interest. In particular, I'm thinking about the details of NSA efforts to infiltrate and corrupt the standards setting groups that produce commercial crypto schemes.

But the rest of it is a lot more dubious. It's not clear to me how disclosing NSA's decryption breakthroughs benefits the public debate much, unlike previous disclosures that have raised serious questions about the scope and legality of NSA's surveillance of U.S. persons. Conversely, it's *really* easy to see how disclosing them harms U.S. efforts to keep up our surveillance on genuine bad guys. Unlike previous rounds of disclosures, I'm a lot less certain that this one should have seen the light of day.