SWCP Portal
January 2014

Who watches the watchers?

Can the Internet be Fixed?

Undoubtedly, the most critical issue facing the global online community in 2014 is that of government **Internet surveillance**, particularly by the National Security Agency. The debate that former NSA contractor and whistleblower **Edward Snowden** wanted with his release of classified documents since last June is now in full flower.

Congress is asking pointed questions, two federal judges have issued contradictory opinions regarding the basic legality of key programs, and a presidential commission has made 46 recommendations about known projects. But every day brings new revelations of the extent of government spying that go beyond anything previously imagined. The issues will likely go to the Supreme Court and be thoroughly chewed by Congress before it's over.

Citizens trying to make sense out of all this are being bombarded by wildly-conflicting claims from both sides. They sound like arguments coming from different planets. Just what is going on anyway behind all the smoke and mirrors and crazy talk? How does all this affect the average person just trying to get by with their online lives?

The questions

How this will all play out and what ultimate effect it will have on the Internet cannot yet be foreseen. But what we know so far can be summed up by a handful of basic questions and a few general conclusions.

1. Has NSA Internet data collection and surveillance actually prevented terrorist attacks?

The current situation was forged in the wake of 9/11 with the **Patriot Act**, but this most crucial question of all is surprisingly hard to answer. While the NSA would love to take credit for preventing a repeat of that horrible day, there are very few concrete examples of foiled plots that the agency can point to: when pressed, Gen. Alexander, the head, could cite only one, whereas neither the judge who thought the phone-data collection program was unconstitutional nor the President's commission could find any.

2. How much spying is really going on?

Before Snowden, it generally appeared as if the Chinese, Russians, and criminal syndicates were the major parties interested in breaking into computer systems. We can be confident now that the US effort easily matches and probably far exceeds them. Our hackers seem to be the best.

However, Glenn Greenwald, a reporter dealing closely with Snowden, said recently that *only* 1% of his material has been released. Even if most will never be, there could well be plenty more bombshells to come. While Director of Intelligence Clapper has admitted to lying to Congress, the NSA hides behind a blizzard of silly **code names** and very carefully phrased answers. So when he said that the NSA did *not* spy on Americans with the phone metadata collection program, he was technically correct – but there are *plenty* of other tools the NSA could, can, and does use.

3. What is the extent and purpose of the spying?

The NSA claims they're busy **preventing terrorism**, yet they spied on German Chancellor Angela Merkel's phone calls. They have also spied on a Belgian telecommunications firm and a Brazilian oil company for reasons seemingly unrelated to keeping the homeland safe.

The technical abilities the NSA possesses are truly mind-blowing. Just a few months ago, you would have been laughed at – or thought crazy – if you claimed files had been somehow planted on your machine, that your web-camera was watching you without your knowledge or consent, that spies planted bugs in your new computer and cellphone during shipping, and your screen was beaming signals on its own. Yet, all these things and many more have been now documented as off-the-shelf exploits of the NSA. Reality is hard to tell from paranoia these days.

And yes, the target can be *anyone*. If for example, a friend of a friend of yours is tagged as having talked to a certain foreign phone number, and if they decide the chances of

Continued on back

Continued from front

him or her being an American are less than 50%, then not only *all* that person's calls, but *all* of his or her friends and *all* their contacts will be automatically checked, too – including *you*, of course. If each person involved has say, 50 contacts, then *125,000 people* will be scrutinized, all due to just a *single* telephone call.

4. Will reforms do any good?

Ultimately, **international treaties** may attempt to post limits on surveillance. But spying is as much of the human condition as war, so it will doubtless continue to some degree. And when dealing with secret agencies, *no* amount of official oversight may be sufficient.

We know because it's *already happened*. The NSA's plan to spy on *everyone* was first revealed after 9/11 under the all-too-honest project name "*Total Information Awareness*" complete with an unfortunate logo of an eye in a pyramid overlooking the planet. Congress balked at the idea, but the NSA went ahead anyway without the creepy identity, so Congress actually cut funding for it. The NSA just made the program top-secret and moved it into the black realm.

The results

The National Security Agency are surely *not* the only spies on the Net, and doubtless *somebody* needs to keep the Internet safe. The issue of government surveillance would have surfaced eventually, but the manner in which it has may completely alter our expectations of the future development of the Internet. The reason to doubt is that the NSA apparently hasn't been making it safer, but rendering the Net much more dangerous for all parties. Here's how:

1. The Internet may be fundamentally broken.

The damage is not apparent: everything runs just as it always has, and there's little indication that anything is amiss. But the Net is *not* powered by electricity. It runs entirely on **trust**, which is its greatest flaw as well as its greatest strength. The tacit agreements between users and providers have been under assault almost from the very beginning by spammers, hackers, and spies. The traumatic realization of their final shattering cannot be overstated. This disillusionment may be a necessary phase of growing up, but it won't be easy to get through.

2. Surveillance will subtly change everything.

Historians will note the strange irony that the very creators of the Internet – the American military-industrial complex – were also the ones that finally broke it. Which explains the stated desire of the spy agency's supporters and former directors to hang Snowden from a tree. Their rage comes largely from their knowledge that just as in atomic physics, with humans, *observation changes behavior.*

Now that people *know* they are being watched, their activities are morphing, making the spooks' work much harder. They switch to search engines that won't identify them like **DuckDuckGo** and **encrypt email**. Google, Yahoo, Microsoft, and other tech giants who willingly cooperated with the NSA but were spied on anyway, also are encrypting their internal communications in desperate efforts to stem the loss of hundreds of billions of dollars from foreign companies. And that is just the beginning.

Hardware and software from the servers that supply content and provide firewalls guarding big corporate networks to smartphones and web-browsers are all coming under increasing scrutiny for security. The value of the cloud itself is being questioned. Non-hierarchical network topologies, such as **mesh networks** which don't depend on vertical relationships and centralization are suddenly under serious discussion and spying is one reason why.

Open-source software will become more widespread than ever as it is deemed more trustworthy. Perhaps the entire model that the commercial use of the Net is based on, a system of users trading data for Internet services, will be modified due to suspicions of how that data is used.

The Internet was envisioned to be free and open from end to end. Now it may become **balkanized**, fractured into "*splinternets*," walled national or corporate realms. Like corporations, foreign powers including Brazil and Germany are talking about building their own private networks to keep data safely at home due to targeting by the NSA.

3. The cure may be worse than the disease.

Not only have American businesses lost a huge treasury of trust and goodwill, both foreign and domestic, that may never be regained. American Net dominance is *over*. Many now feel that the US has shown itself to be a **bad steward** of the Internet, and the UN or some other body will probably have to assume ultimate governing authority over it.

Possibly most alarming of all, in its lust for data, the NSA has made the Internet less safe for *everyone*. They have worked to **weaken encryption**, and found or been informed in advance of hundreds of **security flaws** in software which they have determined to keep secret for as long as possible. In the meantime, those holes are being found and exploited by criminals and foreign powers.

Worst of all, the NSA has actively **weaponized the Net**. By accessing the Internet backbone, they can take over machines remotely. Only by encrypting *all* connections can this be prevented. And with the **Stuxnet virus** used against Iran, they have shown the world how to destroy industrial machinery over the Net. The agency now warns of **cyberwar**, a threat for which they bear much responsibility. But at least that can be counted on to keep them in business for a long time to come.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-243-SWCP (7927) ◉ **SWCP.com** ◉ **Help@swcp.com**

5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**