*[Ed. note: For more information on these topics, please click on the **blue links** to access the original webpages in your browser.]*

The Spooks in the Machines

October is here, when days turn cool, nights lengthen, and fallen leaves rustle in darkening shadows. Halloween is coming; a time for ghost stories and tales of monsters lurking in the gloom around us to frighten young imaginations. Yet this year, some real and scary stories have come out that could give us grown-ups sleepless nights, too.

These news reports and leaks are about ogres and heroes: groups bent on destruction and control and those who are fighting them. The problem is that, these stories being for adults, it's sometimes hard to tell which is which.

Central to these narratives is the **National Security Agency** or **NSA**. Their mission is necessary in our modern world as it is concerned with foreign intelligence gathering, code-breaking, and computer security. The Agency is expressly forbidden to spy on American citizens, and their primary purpose now is to prevent terrorism. The spy agency is so secret that its initials were once humorously said to mean "*No Such Agency*." But few laugh now, for very serious questions have been raised about the universal extent of their spying and what it's really all about.

Welcome to the Machine

Leaks have been going on for years. But starting this spring with dribbles from **Wikileaks** and **Anonymous**, the revelations have climaxed with the exposure by former contractor **Edward Snowden** of the vast array of code-named data-gathering programs deployed by the NSA. These still-ongoing leaks of the massive amount of Internet surveillance and data-mining by the spy agency have entirely changed our picture of the Net and how it works. This has forced information directly from the feds to **defend** their practices – and lobby for even *more* powers.

These programs are hidden behind codenames like **STELLAR WIND** and **MAINWAY**, fenced in with bureaucratic double-speak. But enough has come out to permit speculation on what it might mean, and how it all could affect our online future. The outlook is certainly foreboding, and like in the best horror stories, there is hope – but a happy outcome is not guaranteed. That however, will be the subject of a future issue of the *Portal*. First, it is necessary to try to get a handle on just what has been going on so far.

Many of Edward Snowden's revelations concern the NSA's role in spying on foreigners. Snowden maintains he would not disclose anything that might harm these legitimate efforts, so there is nothing on the agency's attempts to penetrate Russia or **China**. There's no mention of **cyber-war** or the **Stuxnet virus** either. Yet even so, the revelations have been shocking as to who has been targeted.

TOTAL INFORMATION AWARENESS
STUXNET | STELLAR WIND | ECHELON
PROMIS | BOUNDLESS INFORMANT
DROPMIRE | THINTHREAD | FAIRVIEW
BLARNEY | PINWALE
BULLRUN | OLIVE
MARINA | ARET
RAGTIM | BASH
KLONDYKE | SHE EDIDO
EGOTISTICAL GIRAFFE | STREAM
X-KEYSTROKE | PRISM | MAINWAY
SURVEILLANCE DETECTION UNIT
PRESIDENT'S SURVEILLANCE PROGRAM

The US has even bugged our allies: for instance, both **India**'s UN mission and embassy, and **Brazil**. In the latter case, the giant oil company Petrobus was the target – and seemingly not for counter-terrorism but industrial espionage. This has angered Brazilians to the point where they are talking about building their own **national Internet**.

The Belgian telecom giant **Belgacom**, which had been hacked for two years, turned out to have been done by the NSA's British counterpart **GCHQ**. However, the documents show that the two agencies have a remarkably close relationship, and that one often does the dirty work for the other when legal or other restrictions get in the way. (The NSA spies on, but also shares many things, with **Israel**.)

It gets much more ominous on the domestic side. Officially known as the "**President's Surveillance Program**," it supposedly started shortly after 9/11. However, former Qwest CEO, Joseph Nacchio, after being released from prison for insider trading, **alleged** that he was jailed due to his company being the sole telecom to refuse to give up their phone records a whole *6 months before* the attack.

After September 11, then-President George W. Bush **authorized** the agency under the color of law to conduct surveillance within the US without warrants or oversight. Though less than 1000 al Queda sympathizers were suspected to be in our country, the programs caught up millions of unsuspecting citizens as well. First the NSA acquired all **call-detail records** from AT&T, MCI, and Sprint among others. Along with this, they constructed **secret rooms** in switching centers to suck down and analyze content and data in real time straight from the tubes.

The **objective** was simply to create a database of every call made in the country. After being revealed in 2005, the voluntary agreements were changed to court orders. But it wasn't until the **Verizon order** was leaked this year that the extent was grasped. Director of National Intelligence James Clapper at first **claimed** that their soaking up all phone records is not concerned with *content* – the data – but the time, length, and number called – the data *about* the data, or **metadata**. He said it is *not* spying on citizens.

Yet, since metadata reveals connections between people, places, and times, it can **reveal** even more sometimes than the actual content. Secondly, metadata is also susceptible to misinterpretation. To prevent that, acquiring even more becomes necessary. So the **internal rules** restricting targeting are fudged. Americans are not supposed to be spied on – unless the person talked to is outside the country. Or if the Agency gets their **area code wrong**. Believe it or not, that was what they claimed happened when they were caught spying on people in Washington, DC.

Once a person is of interest, all of his or her connections are checked too: up to **three degrees** out just to be sure. Mathematically, this is not *quite* far enough from anyone to haul in both Kevin Bacon and the pope for scrutiny. Though spokespersons still refuse to definitely say whether or not the NSA collects the actual *content* of all phone calls made in the country, Gen. Keith Alexander, the head of the Agency, **says** he wants them. Some observers think that its data-storage centers, such as the new $2 billion one in **Utah** which opened **despite** the government shutdown, are so huge that they must be storing calls.

The Agency has **admitted** that they've tested their ability to track cell-phone users' locations. In any case, the sweep of their collections is so **broad** that millions of Americans have been caught up in their net too. But their reach goes far beyond phone calls. Through a program named **PRISM**. they also have had access since 2007 to the servers of Google, Facebook, Yahoo, Paypal, YouTube, Skype, AOL, and Apple, as well as directly to the **Internet backbone**.

The rationale seems to be that to find the needle in the haystack the NSA must own the entire pile. It seems they've got it, too. What the confusing batch of James Bond codenames for programs and capabilities boils down to is this: *the spooks can see just about* **everything**: *what you post on the Web, what email you send and receive, what you look for, every site you visit and what you download.* Whether you have nothing to hide or everything, your data is being scooped up with everyone else's.

Your computer's **operating system** likely came with backdoors already installed. **Encryption standards** may be compromised. If the NSA **serves** a provider for your files, not only must the service provider comply, but could face jail time if they even let *anyone* know. This is why the companies mentioned above all seem so shocked to find about these programs, why they then asked for permission from the court to talk, and why Snowden's encrypted email provider was **busted** the day after he went public.

Companies are given positive incentives to cooperate also. They are **paid millions** for their services, just as the phone companies charge handsome fees for wiretapping. But as the Qwest and other cases show, there are other advantages for getting in bed with the government, such as preferential treatment and insider information.

The All-Seeing Eye

Why all this is so disturbing is best illustrated by one program originally called **Total Information Awareness**. First publicly proposed in 2002, the program called for pulling together *all* online information of *everyone* in the US to track their social networking – kind of a spooky Facebook. Though 9/11 was still painfully fresh, the proposal was quickly defeated in Congress, possibly because the logo showed the eye in the pyramid from the dollar bill scanning the planet. So the NSA dropped the graphic, changed the name from "*Total*" to "*Terrorism*" and tried again.

This time, Congress denied it funding, so it went entirely undercover. In 2010, the Agency was allowed to analyze huge sets of metadata "*for foreign intelligence purposes*" without bothering to check whether Americans were included. By the next year, they **implemented** basically what they'd wanted for a decade or more. The spooks always somehow get what they desire no matter what.

The real question is *why*. There's **little evidence** that any of this has actually stopped any attacks. Tied with that is the most troublesome fact of all: **the NSA lies**. While no-one expects a spy agency to be candid with the public, they have kept their supposed judicial and legislative overseers in the dark, too. Even the secret FISA courts which normally rubber stamp their requests have **criticized** them for **lying to them** on more than one occasion.

Time and again the Agency has made claims that they soon had to back away from. Claims like that there was strict oversight of each request, when there is just a line to be filled in on the **form**. Or that no mistakes were made when an **internal audit** showed thousands of errors.

The Agency **said** they only spied to prevent terrorism, but did so on Brazil's oil company for economic reasons. They even claimed that no-one had ever used the system for personal gain. Yet they had a program called **LOVEINT** just to catch agents who spied on romantic interests. With few real safegaurds, the temptation for abuse of these awesome powers is high and the overall pattern is **worrisome**.

Sen. Ron Wyden (D-Or) **said** to the face of NSA chief Alexander that "*the leadership of NSA built an intelligence collection system that repeatedly deceived the American people*."

So if you're feeling strangely paranoid as if you're being followed, it may not be due to the season, and you may not be wrong. There *are* spooks lurking in the machine and they *are* watching you. But at least you're not alone.

Future issues will discuss who else is watching us, the costs and effects of all this surveillance, and what, if anything, can or should be done.

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