CELEBRATING 20 YEARS OF SERVICE 1994-2014

SWCP Portal

October 2014

Ever get that feeing like somebody's watching you?

The Watchlists of Terror

Halloween is a time for scary stories, spine-tingling tales to keep you awake listening for noises in the night. There's no shortage of real monsters to fear these days, and the Internet, with zombie computers, hackers, identity thieves, and malware can easily provide sufficient anxiety to assure sleeplessness.

A peril that may be just as frightening is being held as helplessly trapped as a fly in a spider's web in a situation that targets you like a drone, scrutinizes your online life, and can deny you the ability to travel and make a living. Even more scary, this fate could befall you or *any* user no matter how innocent or canny – and you might not realize or be able to fight it either.

This is what could theoretically happen to you if you should somehow arouse the suspicions of the **National Security Agency**. It puts you in a paranoid, powerless nightmare straight out of Kafka resulting in a situation as awful as in any macabre tale by Poe.

Even the dead are watched

The US government maintains several lists of people it thinks need watching. The "**No-Fly**" list, which lists people forbidden to travel on commercial aircraft, is the most well-known, but there are others, including a "**Selectee**" list, which triggers enhanced screening at airports and borders. But the main list is the FBI's "**Terrorist Screening Database"**, targeting *680,000* individuals, both citizens and foreigners alike.

For law-abiding Americans, the terrifying thing about these lists is that it is easy to get on and nearly impossible to get off. The standards to be identified as a "known" or "suspected" terrorist are based on "**reasonable suspicion**" which means a single tweet or Facebook posting could land you on it. Courts have ruled that simply avoiding eye contact with an officer, traveling alone, or at night, all amount to reasonable suspicion. Concrete facts are *not* necessary: a hunch or feeling by a nameless official is all it takes.

Over *60%* on the list have no known affiliation with a terrorist group. You can fall victim to it simply by having a name similar to that of a suspect. In 2004, the late **Senator Ted Kennedy** complained that he was forbidden to fly on *5* different occasions. Along with the president of Bolivia, infants as young as *2* have been stopped or frisked. And since terrorists may use false identities, even dying won't set you free. In fact, **rules** permit names of dead spouses of suspected terrorists to be added *after* they have passed on.

Your living family members are also automatically watchlisted, along with your friends and associates. But surveillance can extend far beyond anyone you know. A single official could decide to put *entire categories* of people on the No-Fly and Selectee lists.

Though the government's rulebook is unclassified, the Administration tried to keep the guidelines secret anyway as the rules are complicated, confusing, and full of exceptions and judgment calls. Since you can be suspected of terrorism by mere suspicion of associating with other suspects, the entire system is based on the very dubious premise of "**pre-crime**": that with enough information it could predict who *might* commit a terrorist act some time in the future.

National security seems less endangered by such revelations than the inefficiencies and absurdities involved in determining targets. Along with bombing, assassination, and hijacking, their broad definition of terrorist activity includes destruction of

Continued on back

Continued from front

government property and damaging computers used by financial institutions among other offenses.

In 2009, the list failed to prevent the Nigerian underwear bomber who was on it from boarding a plane. The president responded by increasing the powers of agencies to place names on the list and the pressure to do so. But three years later, the Government Accounting Office noted there was *still* no agency responsible for screening or vetting the database.

Guidelines were revised and expanded two years after that, but the system remains without checks and balances. In 2013, officials nominated *468,749* names for inclusion, only *4,915* of which were rejected – about *1%*. So much for the principles of "due process" and "innocent until proven guilty."

Under the magnifying glass

Once targeted, *any* interaction you have with authorities can be used as an opportunity to collect your data. Information from fingerprints to gun licences, IDs, travel plans, prescriptions, cellphones, bank cards, email addresses, thumb drives, iPods, Kindles, cameras, and so on will be sought. Business cards, scuba gear, binoculars, books and their condition, even jewelry and pets will be noted. All your private information can then be accessed through **ICREACH**, the NSA's Google-like search engine, by *23* government agencies, while the Terrorist Database is also shared with at least *22* foreign governments.

Once the US government lists you as a suspected terrorist, the consequences are severe and widespread, for *all* other informed governments and agencies treat you as one, too. This can make it impossible to travel, and difficult to find a job and stay out of jail, for even the most routine encounter with law enforcement can then become a dangerous ordeal.

Even if stopped for speeding, your name will be **queried**. The officer then knows he's dealing with a potential terrorist and menace to public safely. Given recent deadly instances of armed overreaction by police, this is *not* a situation guaranteed to end well.

Your online life, including web-browsing, email, and social networking will be an open book to the NSA, which Edward Snowden's **leaks** show can "own" you in more ways than can be counted. If they want to hack your devices or accounts, they can and will. Even buying a new computer won't help, as they could intercept it during shipping and bug it.

Like their **British counterparts**, however, they could wreck your online life. They can change Google rankings of your website, alter Facebook stats, even create false posts in your name to destroy your reputation as they track your online habits and hangouts. If they come across evidence of illegal activities, they can quietly (and illegally) alert the appropriate authorities without giving the game away. They likely have the technical abilty to plant files, too, though there's no evidence that this has actually been done.

For living people, getting off the list is simple but not clear. You file a complaint through the Department of Homeland Security's **Traveler Redress Inquiry Program**. Their internal review is secret and not subject to judicial oversight. Only if *all* the agencies who've contributed information about you agree could this result in your removal from the list or a change in status; yet whatever the result, you will *not* be informed.

If you are put on the No-Fly list while abroad, you *might* be able to get a one-time waiver through a US embassy or consulate to return, but you won't know you're still on the list until the *next* time you try to fly.

Americans in these fearful times seem willing to take all this without complaint *if* it keeps us safe. As long as there are no more 9/11s, we seem content to tolerate any affront to liberty, "better safe than sorry." But there are many **ways** this could go horribly wrong. Failure to stop an attack is just one of them.

Increased Disk Storage for Everyone

We just bought a large disk-server and so are generously increasing disk quotas for all our members by at least *250%*. This will allow much more room to save email online for those without web-hosting plans. For web-publishers, the extra space now available is simply humongous. Here's the breakdown:

Shell or POP Accounts without a web-hosting plan:
Was *20MB*, now *50MB* (*2.5x* more)

Starter Websites: Was *20MB*, now *50MB* (*2.5x* more)

Basic Websites: Was *200MB*, now *1GB*
(*800MB* or *5x* more)

Pro Websites: Was *2GB*, now *10GB* (*8GB* or *5x* more)

All users' disk allocations have already been increased, and migration to the new servers is ongoing.

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**
Click on blue heads in PDF file to access links.