GlobalResearch
Center for Research on Globalization

The Government's Mass Spying Is An Affront To Democratic Values

Let's Also Not Pretend It's An Effective And Efficient Way Of Keeping Us Safe

By Washington's Blog
Global Research, June 29, 2013
Washington's Blog

Region: USA
Theme: Intelligence, Police State & Civil Rights

Top Terrorism Experts Say that Mass Spying Doesn't Work to Prevent Terrorism

Never mind the fact that – if the government's spying was really only aimed at protecting us from terrorism – the NSA probably wouldn't put so many resources into spying on our allies at the G20 summit, the European Parliament or Chinese universities (or perhaps even our own government officials).

America's terrorism experts say that the NSA's mass surveillance program *doesn't* make us safer.

An article on Bloomberg notes that real terrorists don't even *use* the normal phone service or publicly-visible portions of the web that we innocent Americans use:

> The debate over the U.S. government's monitoring of digital communications suggests that Americans are willing to allow it as long as it is genuinely targeted at terrorists. What they fail to realize is that the surveillance systems are best suited for gathering information on law-abiding citizens.
>
> ***
>
> The infrastructure set up by the National Security Agency, however, may only be good for gathering information on the stupidest, lowest-ranking of terrorists. The Prism surveillance program focuses on access to the servers of America's largest Internet companies, which support such popular services as Skype, Gmail and iCloud. These are not the services that truly dangerous elements typically use.
>
> In a January 2012 report titled "Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age," the Dutch General Intelligence and Security Service drew a convincing picture of an Islamist Web underground centered around "core forums." These websites are part of the Deep Web, or Undernet, the multitude of online resources not indexed by commonly used search engines.
>
> The Netherlands' security service, which couldn't find recent data on the size of the Undernet, cited a 2003 study from the University of California at Berkeley as the "latest available scientific assessment." The study found that just 0.2 percent of the Internet could be searched. The rest remained inscrutable and has probably grown since. In 2010, Google Inc. said it had indexed just 0.004 percent of the information on the Internet.
>
> Websites aimed at attracting traffic do their best to get noticed, paying to

> tailor their content to the real or perceived requirements of search engines such as Google. Terrorists have no such ambitions. They prefer to lurk in the dark recesses of the Undernet.
>
> "People who radicalise under the influence of jihadist websites often go through a number of stages," the Dutch report said. "Their virtual activities increasingly shift to the invisible Web, their security awareness increases and their activities become more conspiratorial."
>
> ***
>
> Communication on the core forums is often encrypted. In 2012, a French court found nuclear physicist Adlene Hicheur guilty of, among other things, conspiring to commit an act of terror for distributing and using software called Asrar al-Mujahideen, or Mujahideen Secrets. The program employed various cutting-edge encryption methods, including variable stealth ciphers and RSA 2,048-bit keys.
>
> ***
>
> Even complete access to these servers brings U.S. authorities no closer to the core forums. These must be infiltrated by more traditional intelligence means, such as using agents posing as jihadists or by informants within terrorist organizations.
>
> Similarly, monitoring phone calls is hardly the way to catch terrorists. They're generally not dumb enough to use Verizon.
>
> ***
>
> At best, the recent revelations concerning Prism and telephone surveillance might deter potential recruits to terrorist causes from using the most visible parts of the Internet. Beyond that, the government's efforts are much more dangerous to civil liberties than they are to al-Qaeda and other organizations like it.

The top counter-terrorism czar under Presidents Clinton and Bush – Richard Clarke – notes:

> The argument that this sweeping search must be kept secret from the terrorists is laughable. Terrorists already assume this sort of thing is being done. Only law-abiding American citizens were blissfully ignorant of what their government was doing.
>
> ***
>
> If the government wanted a particular set of records, it could tell the Foreign Intelligence Surveillance Court why — and then be granted permission to access those records directly from specially maintained company servers. The telephone companies would not have to know what data were being accessed. There are no technical disadvantages to doing it that way, although it might be more expensive.
>
> Would we, as a nation, be willing to pay a little more for a program designed this way, to avoid a situation in which the government keeps on its own computers a record of every time anyone picks up a telephone? That is a question that should have been openly asked and answered in Congress.

William Binney – the head of NSA's digital communications program – says that he set up the NSA's system so that all of the information would automatically be *encrypted*, so that the government had to obtain a search warrant based upon probably cause before a particular suspect's communications could be decrypted. But the NSA now collects all data in an *unencrypted* form, so that no probable cause is needed to view any citizen's information. He says that it is actually cheaper and easier to store the data in an encrypted format: so the government's current system is being done for political – *not practical* – purposes. Binney's statements have been confirmed by other high-level NSA whistleblowers.

Binney also says:

- Massive surveillance doesn't work to make us safer
- The government is using information gained through mass surveillance in order to go after anyone they take a dislike to (a lieutenant colonel for the Stasi East German's agrees)

Israeli-American terrorism expert Barry Rubins notes:

> What is most important to understand about the revelations of massive message interception by the U.S. government is this:
>
> In counterterrorist terms, it is a farce. Basically the NSA, as one of my readers suggested, is the digital equivalent of the TSA strip-searching an 80 year-old Minnesota grandmothers rather than profiling and focusing on the likely terrorists.
>
> ***
>
> And isn't it absurd that the United States can't ... stop a would-be terrorist in the U.S. army who gives a power point presentation on why he is about to shoot people (Major Nadal Hassan), can't follow up on Russian intelligence warnings about Chechen terrorist contacts (the Boston bombing), or a dozen similar incidents must now collect every telephone call in the country? A system in which a photo shop clerk has to stop an attack on Fort Dix by overcoming his fear of appearing "racist" to report a cell of terrorists or brave passengers must jump a would-be "underpants bomber" from Nigeria because his own father's warning that he was a terrorist was insufficient?
>
> And how about a country where terrorists and terrorist supporters visit the White House, hang out with the FBI, advise the U.S. government on counter-terrorist policy (even while, like CAIR) advising Muslims not to cooperate with law enforcement....
>
> ***
>
> Or how about the time when the U.S. Consulate in Jerusalem had a (previously jailed) Hamas agent working in their motor pool with direct access to the vehicles and itineraries of all visiting US dignitaries and senior officials.
>
> ***
>
> Suppose the U.S. ambassador to Libya warns that the American compound there may be attacked. No response. Then he tells the deputy chief of mission that he is under attack. No response. Then the U.S. military is not allowed to

> respond. Then the president goes to sleep without making a decision about doing anything because communications break down between the secretaries of defense and state and the president, who goes to sleep because he has a very important fund-raiser the next day. But don't worry because three billion telephone calls by Americans are daily being intercepted and supposedly analyzed.
>
> In other words, you have a massive counterterrorist project costing $1 trillion but when it comes down to it the thing repeatedly fails. In that case, to quote the former secretary of state, ""What difference does it make?"
>
> If one looks at the great intelligence failures of the past, these two points quickly become obvious. Take for example the Japanese surprise attack on Pearl Harbor on December 7, 1941. U.S. naval intelligence had broken Japanese codes. They had the information needed to conclude the attack would take place. [Background.] Yet a focus on the key to the problem was not achieved. The important messages were not read and interpreted; the strategic mindset of the leadership was not in place.
>
> ***
>
> And remember that the number of terrorists caught by the TSA hovers around the zero level. The shoe, underpants, and Times Square bombers weren't even caught by security at all and many other such cases can be listed. In addition to this, the U.S.-Mexico border is practically open.
>
> **
>
> The war on al-Qaida has not really been won, since its continued campaigning is undeniable and it has even grown in Syria, partly thanks to U.S. policy.
>
> ***
>
> So the problem of growing government spying is three-fold.
>
> –First, it is against the American system and reduces liberty.
>
> –Second, it is a misapplication of resources, in other words money is being spent and liberty sacrificed for no real gain.
>
> –Third, since government decisionmaking and policy about international terrorism is very bad the threat is increasing.

(And see this.)

Mass Spying Actually HURTS – Rather than Helps – Anti-Terror Efforts

Not yet convinced?

Former NSA executive William Binney – who was the *head* of the NSA's entire digital spying program – told Daily Caller that the spying dragnet being carried out by the government is less than useless:

> Daily Caller: So it seems logical to ask: Why do we need all of this new data collection when they're not following up obvious leads, such as an intelligence agency calling and saying you need to be aware of this particular terrorist?

> Binney: It's sensible to ask, but that's exactly what they're doing. They're making themselves dysfunctional by collecting all of this data. They've got so much collection capability but they can't do everything.
>
> ***
>
> [All this data gathered is] putting an extra burden on all of their analysts. It's not something that's going to help them; it's something that's burdensome. There are ways to do the analysis properly, but they don't really want the solution because if they got it, they wouldn't be able to keep demanding the money to solve it. I call it their business statement, "Keep the problems going so the money keeps flowing." It's all about contracts and money.
>
> ***
>
> The issue is, can you figure out what's important in it? And figure out the intentions and capabilities of the people you're monitoring? And they are in no way prepared to do that, because that takes analysis. That's what the big data initiative was all about out of the White House last year. It was to try to get algorithms and figure out what's important and tell the people what's important so that they can find things. The probability of them finding what's really there is low.

Indeed, even before 9/11 – when Binney was building the precursor to the NSA's current digital collection system – there weren't enough analysts to look through the more modest amount of data being collected at the time:

> The danger of the mass collection of data by the NSA is that it "buries" analysts in data, said Binney, who developed a surveillance program called ThinThread intended to allow the NSA to look at data but not collect it. The NSA dumped that program in favor of more extensive data collection.
>
> "The biggest problem was getting data to a manageable level," he said. "We didn't have enough people, we couldn't hire enough people east of the Mississippi to manage all the data we were getting."

Terrorism expert Barry Rubins writes:

> There is a fallacy behind the current intelligence strategy of the United States, the collection of massive amounts of phone calls, emails, and even credit card expenditures, up to 3 billion phone calls a day alone, not to mention the government spying on the mass media. It is this:
>
> The more quantity of intelligence, the better it is for preventing terrorism.
>
> In the real, practical world this is—though it might seem counterintuitive—untrue. You don't need–to put it in an exaggerated way–an atomic bomb against a flea. The intelligence budget is not unlimited, is it? Where should hiring priorities be put?
>
> ***
>
> It is not the quantity of material that counts but the need to locate and correctly understand the most vital material. This requires your security forces

to understand the ideological, psychological, and organizational nature of the threat.

***

If the U.S. government can't even figure out what the Muslim Brotherhood is like or the dangers of supporting Islamists to take over Syria, or the fact that the Turkish regime is an American enemy, or can't even teach military officers who the enemy is, what's it going to do with scores of billions of telephone call traffic to overcome terrorism? It isn't even using the intelligence material it already has!

If, however, the material is almost limitless, that actually weakens a focus on the most needed intelligence regarding the most likely terrorist threats. Imagine, for example, going through billions of telephone calls even with high-speed computers rather than, say, following up a tip from Russian intelligence on a young Chechen man in Boston who is in contact with terrorists or, for instance, the communications between a Yemeni al-Qaida leader and a U.S. army major who is assigned as a psychiatrist to Fort Hood.

That is why the old system of getting warrants, focusing on individual email addresses, or sites, or telephones makes sense, at least if it is only used properly. Then those people who are communicating with known terrorists can be traced further. There are no technological magic spells. If analysts are incompetent ... and leaders unwilling to take proper action, who cares how much data was collected?

***

Decision-makers and intelligence analysts only have so many hours in the day. There can only be so many meetings; only so many priorities. And the policymaking pyramid narrows rapidly toward the top. There is a point of diminishing returns for the size of an intelligence bureaucracy. Lower-priority tasks proliferate; too much paper is generated and meetings are held; the system clogs when it has too much data.

PC World reports:

"In knowing a lot about a lot of different people [the data collection] is great for that," said Mike German, a former Federal Bureau of Investigation special agent whose policy counsel for national security at the American Civil Liberties Union. "In actually finding the very few bad actors that are out there, not so good."

The mass collection of data from innocent people "won't tell you how guilty people act," German added. The problem with catching terrorism suspects has never been the inability to collect information, but to analyze the "oceans" of information collected, he said.

Mass data collection is "like trying to look for needles by building bigger haystacks," added Wendy Grossman, a freelance technology writer who helped organize the conference.

New Republic notes:

This kind of dragnet-style data capture simply doesn't keep us safe.

> First, intelligence and law enforcement agencies are increasingly drowning in data; the more that comes in, the harder it is to stay afloat. Most recently, the failure of the intelligence community to intercept the 2009 "underwear bomber" was blamed in large part on a surfeit of information: according to an official White House review, a significant amount of critical information was "embedded in a large volume of other data." Similarly, the independent investigation of the alleged shootings by U.S. Army Major Nidal Hasan at Fort Hood concluded that the "crushing volume" of information was one of the factors that hampered the FBI's analysis before the attack.
>
> Multiple security officials have echoed this assessment. As one veteran CIA agent told The Washington Post in 2010, "The problem is that the system is clogged with information. Most of it isn't of interest, but people are afraid not to put it in." A former Department of Homeland Security official told a Senate subcommittee that there was "a lot of data clogging the system with no value." Even former Defense Secretary Robert Gates acknowledged that "we've built tremendous capability, but do we have more than we need?" And the NSA itself was brought to a grinding halt before 9/11 by the "torrent of data" pouring into the system, leaving the agency "brain-dead" for half a week and "[unable] to process information," as its then-director Gen. Michael Hayden publicly acknowledged.
>
> National security hawks say there's a simple answer to this glut: data mining. The NSA has apparently described its computer systems as having the ability to "manipulate and analyze huge volumes of data at mind-boggling speeds." Could those systems pore through this information trove to come up with unassailable patterns of terrorist activity? The Department of Defense and security experts have concluded that the answer is no: There is simply no known way to effectively anticipate terrorist threats.
>
> ***
>
> The FBI's and NSA's scheme is an affront to democratic values. Let's also not pretend it's an effective and efficient way of keeping us safe.

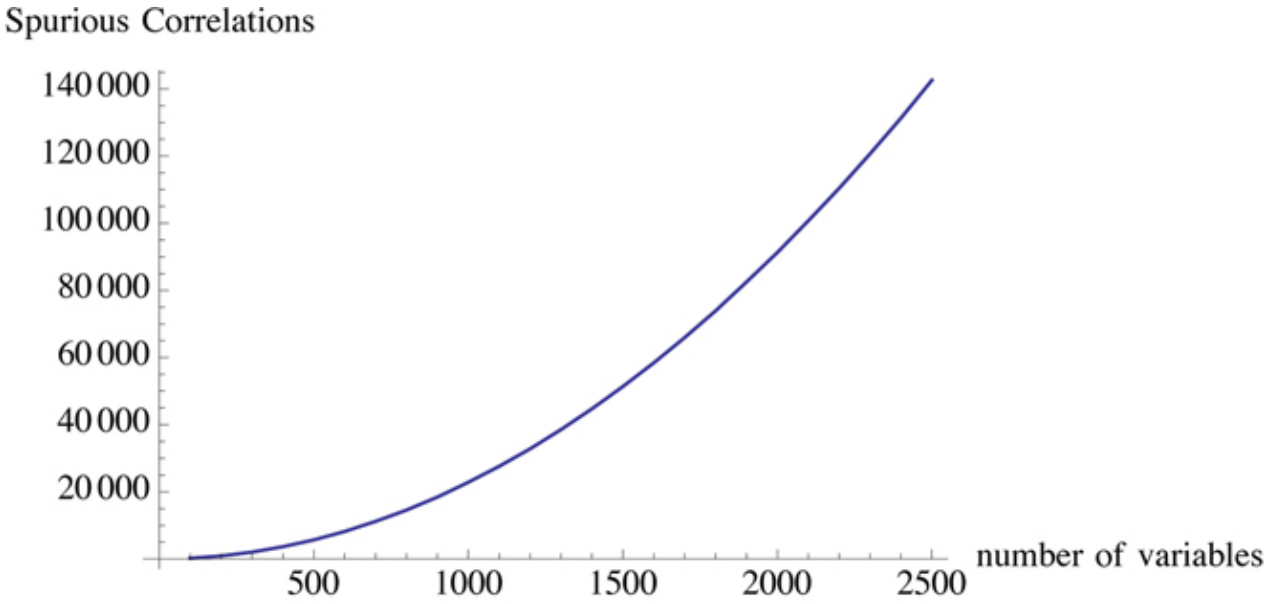
Fortune notes that the NSA's "big data" strategy is ineffective:

> The evidence for big data is scant at best. To date, large fields of data have generated meaningful insights at times, but not on the scale many have promised. This disappointment has been documented in the Wall Street Journal, Information Week, and SmartData Collective.
>
> ***
>
> According to my firm's research, local farmers in India with tiny fields frequently outperform — in productivity and sustainability — a predictive global model developed by one of the world's leading agrochemical companies. Why? Because they develop unique planting, fertilizing, or harvesting practices linked to the uniqueness of their soil, their weather pattern, or the rare utilization of some compost. There is more to learn from a local Indian outlier than from building a giant multivariate yield prediction model of all farms in the world. The same is true for terrorism. Don't look for a needle in a giant haystack. Find one needle in a small clump of hay and see whether similar clumps of hay also contain needles.
>
> You need local knowledge to glean insights from any data. I once ran a data-mining project with Wal-Mart (WMT) where we tried to figure out sales patterns in New England. One of the questions was, "Why are our gun sales lower in Massachusetts than in other states, even accounting for the liberal bias of the

> state?" The answer: There were city ordinances prohibiting the sale of guns in many towns. I still remember the disappointed look of my client when he realized the answer had come from a few phone calls to store managers rather than from a multivariate regression model.
>
> So, please, Mr. President, stop building your giant database in the sky and quit hoping that algorithm experts will generate a terrorist prevention strategy from that data. Instead, rely on your people in the field to detect suspicious local patterns of behavior, communication, or spending, then aggregate data for the folks involved and let your data hounds loose on these focused samples. You and I will both sleep better. And I won't have to worry about who is lurking in the shadows of my business or bedroom.

Likewise, Nassim Taleb writes:

> Big data may mean more information, but it also means more false information.
>
> ***
>
> Because of excess data as compared to real signals, someone looking at history from the vantage point of a library will necessarily find many more spurious relationships than one who sees matters in the making; he will be duped by more epiphenomena. Even experiments can be marred with bias, especially when researchers hide failed attempts or formulate a hypothesis after the results — thus fitting the hypothesis to the experiment (though the bias is smaller there).



> If big data leads to more false correlations, then mass surveillance may lead to more *false* accusations of terrorism.
>
> (Just what we need ...)

The original source of this article is Washington's Blog

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Washington's Blog