GlobalResearch
Center for Research on Globalization

Authoritarians Use Paris Terror Attack As Excuse for Power Grab

In the Wake of French Terror, Governments Demand More Mass Surveillance

By Washington's Blog
Theme: Police State & Civil Rights
Global Research, January 17, 2015
Washington's Blog

In the wake of the terror attack on the publication Charlie Hebdo in Paris, governments from around the world are calling for increased surveillance.

But top security experts agree that mass surveillance is ineffective ... and actually makes us *MORE* vulnerable to terrorism.

For example, the former head of the NSA's global intelligence gathering operations – Bill Binney – says that the mass surveillance INTERFERES with the government's ability to catch bad guys, and that the government failed to stop the Boston Bombing because it was *overwhelmed* with data from mass surveillance on Americans.

Today, Washington's Blog asked Binney whether this applied to the Paris attack as well. He responded that it did:

> A good deal of the failure is, in my opinion, due to bulk data. So, I am calling all these attacks a result of "Data bulk failure." Too much data and too many people for the 10-20 thousand analysts to follow. Simple as that. Especially when they make word match pulls (like Google) and get dumps of data selected from close to 4 billion people.
>
> This is the same problem NSA had before 9/11. They had data that could have prevented 9/11 but did not know they had it in their data bases. This back then when the bulk collection was not going on. Now the problem is orders of magnitude greater. Result, it's harder to succeed.
>
> Expect more of the same from our deluded government that thinks more data improves possibilities of success. All this bulk data collection and storage does give law enforcement a great capability to retroactively analyze anyone they want. But, of course,that data cannot be used in court since it was not acquired with a warrant.

The pro-spying NSA chief and NSA technicians confirmed Binney's statement 3 months before 9/11:

> In an interview, Air Force Lt. Gen. Michael Hayden, the NSA's director ... suggested that access isn't the problem. Rather, he said, the sheer volume and variety of today's communications means "there's simply too much out there, and it's too hard to understand."

***

> "What we got was a blast of digital bits, like a fire hydrant spraying you in the face," says one former NSA technician with knowledge of the project. "It was the classic needle-in-the-haystack pursuit, except here the haystack starts out huge and grows by the second," the former technician says. NSA's computers simply weren't equipped to sort through so much data flying at them so fast.

And see this.

High-level NSA whistleblowers J. Kirk Wiebe, Thomas Drake and Russell Tice all say that mass surveillance of one's one people is *never necessary* to protect national security.

Indeed, the NSA *itself* no longer claims that its mass spying program has stopped terror attacks or saved lives. Instead, intelligence spokesmen themselves now claim that mass spying is just an "insurance policy" to give "peace of mind".

U.S. officials in the legislative, judicial and executive branches of government all say that the mass surveillance of our own people is ineffective:

- 3 Senators with *top secret clearance* "have reviewed this surveillance extensively and have seen *no evidence* that the bulk collection of Americans' phone records has provided *any intelligence of value*that could not have been gathered through less intrusive means"

- Another Senator with top secret clearance agrees, and so does the congress member who wrote the Patriot Act, and *more than 100* congress members from both parties

- As does the official panel created by President Obama to review NSA spying, made up of top former White House officials and other government insiders, including the head of counter-terrorism under Clinton and Bush and former deputy CIA director Michael J. Morrell

- NBC News reports:

> A member of the White House review panel on NSA surveillance said he was "absolutely" surprised when he discovered the agency's lack of evidence that the bulk collection of telephone call records had thwarted any terrorist attacks."It was, 'Huh, hello? What are we doing here?'" said Geoffrey Stone, a University of Chicago law professor….
>
> "That was stunning. That was the ballgame," said one congressional intelligence official, who asked not to be publicly identified. "It flies in the face of everything that they have tossed at us."
>
> The conclusions of the panel's reports were at direct odds with public statements by President Barack Obama and U.S. intelligence officials.

- Former president Clinton (and apparently Carter, as well), agree that mass surveillance is unnecessary

- As do the chairs of the 9/11 Commission which was created by Congress and the White House

- As does the counter-terrorism czar under the Clinton and Bush administrations, Richard Clarke. Andsee this

- As does a federal judge (and see this)

And many private sector security experts agree …

Ray Corrigan – senior lecturer in mathematics, computing and technology at the Open University, UK –noted yesterday in New Scientist that mass surveillance isn't the answer:

> Brothers Said and Cherif Kouachi and Amedy Coulibaly, who murdered 17 people, wereknown to the French security services and considered a serious threat. France hasblanket electronic surveillance. It didn't avert what happened.
>
> ***
>
> The French authorities lost track of these extremists long enough for them to carry out their murderous acts.
>
> ***
>
> Surveillance of the entire population, the vast majority of whom are innocent, leads to thediversion of limited intelligence resources in pursuit of huge numbers of false leads. Terrorists are comparatively rare, so finding one is a needle in a haystack problem. You don't make it easier by throwing more needleless hay on the stack.
>
> It is statistically impossible for total population surveillance to be an effective tool for catching terrorists.
>
> ***
>
> Mass surveillance makes the job of the security services more difficult and the rest of us less secure.

Israeli-American terrorism expert Barry Rubins points out:

> 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.

Internationally-recognized security expert Bruce Schneier agrees that mass surveillance distracts resources from effective counter-terror activities.

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.

NBC News reports:

> Casting such wide nets is also ineffective, [security researcher Ashkan Soltani] argues. Collecting mountains and mountains of data simply means that when the time comes to find that proverbial needle in a haystack, you've simply created a bigger haystack."Law enforcement is being sold bill of goods that the more data you get, the better your security is. We find that is not true," Soltani said.
>
> Collecting data is a hard habit to break, as many U.S. corporations have discovered after years of expensive data breaches. The NSA's data hoard may be useful in future investigations, helping agents in the future in unpredictable ways, some argue. Schneier doesn't buy it.
>
> "The NSA has this fetish for data, and will get it any way they can, and get as much as they can," he said. "But old ladies who hoard newspapers say the same thing, that someday, this might be useful."
>
> Even worse, an overreliance on Big Data surveillance will shift focus from other security techniques that are both less invasive and potentially more effective, like old-fashioned "spycraft," Soltani says.

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.

(And see this and this.)

CNN terrorism expert Peter Bergen says that mass surveillance is not needed to stop another 9/11.

Indeed, mass surveillance – which was already in place prior to 9/11 – hasn’t caught a *single* terrorist.

So why do governments want mass surveillance? Are they ignorant that it is counter-productive in stopping terrorism?

Or are they engaging in a 5,000-year old type of power grab?

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