GlobalResearch
Center for Research on Globalization

The Monitoring of Our Phone Calls? Government Spooks May Be Listening

By Washington's Blog
Global Research, December 22, 2013
Washington's Blog and Global Research 27 June 2013

Region: USA
Theme: Police State & Civil Rights

The Obama administration has been caught spying on the Verizon phone calls of tens of millions of Americans. The spying effort specifically targeted Americans living on U.S. soil.

And as NBC News reports:

> NBC News has learned that under the post-9/11 Patriot Act, the government has been collecting records on every phone call made in the U.S.

But the government has sought to "reassure" us that it is only tracking "metadata" such as the time and place of the calls, and not the actual content of the calls.

That claim is patently absurd.

The American government is in fact collecting and storing virtually every phone call, purchases, email, text message, internet searches, social media communications, health information, employment history, travel and student records, and virtually all other information of every American.

Whistleblowers revealed years ago that the NSA was vacuuming up virtually all Internet communications. The Washington Post and Guardian report today that the NSA is tapping directly into the central servers of 9 leading U.S. Internet companies – including Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple, and soon Dropbox – and extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person's movements and contacts over time.

The Wall Street Journal reported today that the NSA spies on Americans' credit card transactions as well.

In fact, *all* U.S. intelligence agencies – including the CIA and NSA – are going to spy on Americans' finances. The IRS will be spying on Americans' shopping records, travel, social interactions, health records and files from other government investigators.

Glenn Greenwald reported in May:

> A seemingly spontaneous admission this week by a former FBI counterterrorism agent provides a rather startling acknowledgment of just how vast and invasive these surveillance activities are.

***

On Wednesday night, [CNN's Erin] Burnett interviewed Tim Clemente, a former FBI counterterrorism agent, about whether the FBI would be able to discover the contents of past telephone conversations between the two. He quite clearly insisted that they could:

> BURNETT: Tim, is there any way, obviously, there is a voice mail they can try to get the phone companies to give that up at this point. It's not a voice mail. It's just a conversation. There's no way they actually can find out what happened, right, unless she tells them?
>
> CLEMENTE: "No, there is a way. We certainly have ways in national security investigations to find out exactly what was said in that conversation. It's not necessarily something that the FBI is going to want to present in court, but it may help lead the investigation and/or lead to questioning of her. We certainly can find that out.
>
> BURNETT: "So they can actually get that? People are saying, look, that is incredible.
>
> CLEMENTE: "No, welcome to America. All of that stuff is being captured as we speak whether we know it or like it or not."

"All of that stuff" – meaning every telephone conversation Americans have with one another on US soil, with or without a search warrant – "is being captured as we speak".

On Thursday night, Clemente again appeared on CNN, this time with host Carol Costello, and she asked him about those remarks. He reiterated what he said the night before but added expressly that "all digital communications in the past" are recorded and stored:

Let's repeat that last part: "no digital communication is secure", by which he means not that any communication is susceptible to government interception as it happens (although that is true), but far beyond that: all digital communications – meaning telephone calls, emails, online chats and the like – are automatically recorded and stored and accessible to the government after the fact. To describe that is to define what a ubiquitous, limitless Surveillance State is.

There have been some previous indications that this is true. Former AT&T engineer Mark Klein revealed that AT&T and other telecoms had built a special network that allowed the National Security Agency full and unfettered access to data about the telephone calls and the content of email communications for all of their customers. Specifically, Klein explained "that the NSA set up a system that vacuumed up Internet and phone-call data from ordinary Americans with the cooperation of AT&T" and that "contrary to the government's depiction of its surveillance program as aimed at overseas terrorists . . . much of the data sent through AT&T to the NSA was purely domestic."

> ***
>
> That every single telephone call is recorded and stored would also explain this extraordinary revelation by the Washington Post in 2010:
>
> > Every day, collection systems at the National Security Agency intercept and store 1.7 billion e-mails, phone calls and other types of communications. ***
>
> Two Democratic Senators, Ron Wyden and Mark Udall, have been warning for years that Americans would be "stunned" to learn what the US government is doing in terms of secret surveillance.

The Atlantic notes:

> TSA's surveillance of our communications is most likely much, much bigger than [metadata]. Technology has made it possible for the American government to spy on citizens to an extent East Germany could only dream of. Basically everything we say that can be traced digitally is being collected by the NSA.
>
> ***
>
> On its face, the document suggests that the U.S. government regularly collects and stores all domestic telephone records," The Week's Marc Ambinder writes of Glenn Greenwald's scoop last night. "My own understanding is that the NSA routinely collects millions of domestic-to-domestic phone records. It does not do anything with them unless there is a need to search through them for lawful purposes." Previous reporting from many outlets suggests that's true."

As the top spy chief at the U.S. National Security Agency – William Binney – explained, the NSA is collecting some 100 billion 1,000-character emails per day, and *20 trillion* communications of all types per year.

Binney says that the government has collected *all* of the communications of congressional leaders, generals and *everyone else in the U.S. for the last 10 years*.

Binney further explains 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 says that if anyone gets on the government's "enemies list", then the stored information will be used to target them. Specifically, he notes that if the government decides it doesn't like someone, it analyzes all of the data it has collected on that person and his or her associates over the last 10 years to build a case against him. This includes whistleblowers, activists or even government insiders ... like the head of the CIA.

Binney's statements are confirmed by other NSA whistleblowers. For example, Huffington Post reports:

> While at the NSA, [Kirk] Wiebe, along with Ed Loomis and Bill Binney, created a computer program that could isolate large amounts of information collected by the NSA while protecting Americans' privacy. But the NSA ignored their program ....
>
> "We had a solution to this entire problem that would have avoided this whole mess," Wiebe said.
>
> Instead, the NSA chose Trailblazer, a multi-billion dollar computer program that was supposed to revolutionize how the agency analyzed communications data. Wiebe, Loomis, Binney and another NSA employee, Thomas Drake, called for an investigation into Trailblazer, citing massive waste and fraud.

The *Other* Types of Spying the Government Is Doing On Us

In addition, the amount of money and effort the government is putting into spying on Americans using *a wide variety of other technologies* tends to discredit any notion that the government is exercising restraint in monitoring our phone calls (which are *already* being tapped) for content.

For example, the government is flying drones over the American homeland to spy on us.

Senator Rand Paul correctly notes:

> The domestic use of drones to spy on Americans clearly violates the Fourth Amendment and limits our rights to personal privacy.

Emptywheel notes in a post entitled "The OTHER Assault on the Fourth Amendment in the NDAA? Drones at Your Airport?":

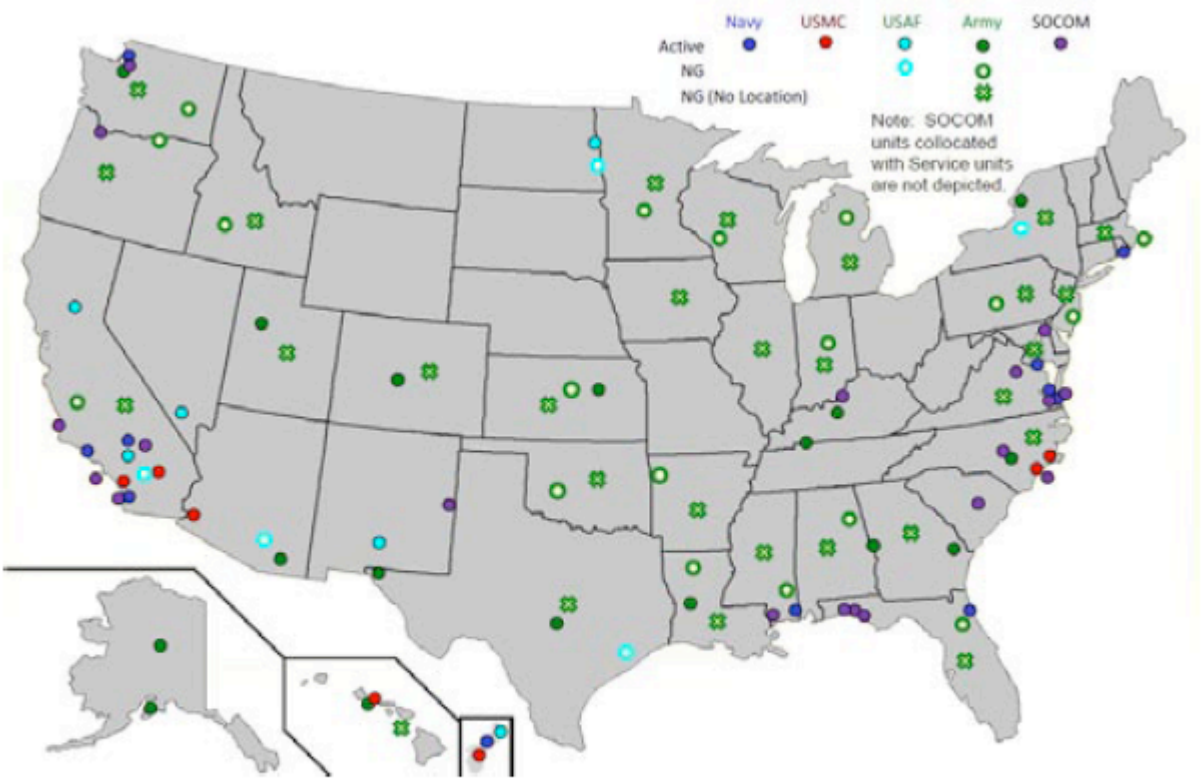

Figure 2: Planned DoD 2015 UAS Locations

> ***
>
> As the map above makes clear–taken from this 2010 report–DOD [the Department of Defense] plans to have drones all over the country by 2015.

Many police departments are also using drones to spy on us. As the Hill reported:

> At least 13 state and local police agencies around the country have used drones in the field or in training, according to the Association for Unmanned Vehicle Systems International, an industry trade group. The Federal Aviation Administration has predicted that by the end of the decade, 30,000 commercial and government drones could be flying over U.S. skies.
>
> ***
>
> "Drones should only be used if subject to a powerful framework that regulates their use in order to avoid abuse and invasions of privacy," Chris Calabrese, a legislative counsel for the American Civil Liberties Union, said during a congressional forum in Texas last month.
>
> He argued police should only fly drones over private property if they have a warrant, information collected with drones should be promptly destroyed when it's no longer needed and domestic drones should not carry any weapons.

> He argued that drones pose a more serious threat to privacy than helicopters because they are cheaper to use and can hover in the sky for longer periods of time.
>
> A congressional report earlier this year predicted that drones could soon be equipped with technologies to identify faces or track people based on their height, age, gender and skin color.

Moreover, Wired reports:

> Transit authorities in cities across the country are quietly installing microphone-enabled surveillance systems on public buses that would give them the ability to record and store private conversations....
>
> The systems are being installed in San Francisco, Baltimore, and other cities with funding from the Department of Homeland Security in some cases ....
>
> The IP audio-video systems can be accessed remotely via a built-in web server (.pdf), and can be combined with GPS data to track the movement of buses and passengers throughout the city.
>
> ***
>
> The systems use cables or WiFi to pair audio conversations with camera images in order to produce synchronous recordings. Audio and video can be monitored in real-time, but are also stored onboard in blackbox-like devices, generally for 30 days, for later retrieval. Four to six cameras with mics are generally installed throughout a bus, including one near the driver and one on the exterior of the bus.
>
> ***
>
> Privacy and security expert Ashkan Soltani told the Daily that the audio could easily be coupled with facial recognition systems or audio recognition technology to identify passengers caught on the recordings.

RT notes:

> Street lights that can spy installed in some American cities
>
> America welcomes a new brand of smart street lightning systems: energy-efficient, long-lasting, complete with LED screens to show ads. They can also spy on citizens in a way George Orwell would not have imagined in his worst nightmare.
>
> With a price tag of $3,000+ apiece, according to an ABC report, the street lights are now being rolled out in Detroit, Chicago and Pittsburgh, and may soon mushroom all across the country.
>
> Part of the Intellistreets systems made by the company Illuminating Concepts, they have a number of “homeland security applications” attached.

> Each has a microprocessor "essentially similar to an iPhone," capable of wireless communication. Each can capture images and count people for the police through a digital camera, record conversations of passers-by and even give voice commands thanks to a built-in speaker.
>
> Ron Harwood, president and founder of Illuminating Concepts, says he eyed the creation of such a system after the 9/11 terrorist attacks and the Hurricane Katrina disaster. He is "working with Homeland Security" to deliver his dream of making people "more informed and safer."

Cell towers track where your phone is at any moment, and the major cell carriers, including Verizon and AT&T, responded to at least 1.3 million law enforcement requests for cell phone locations and other data in 2011. (And – given that your smartphone routinely sends your location information back to Apple or Google – it would be child's play for the government to track your location that way.) Your iPhone, or other brand of smartphone is spying on virtually everything you do (ProPublica notes: "That's No Phone. That's My Tracker").

Fox news notes that the government is insisting that "black boxes" be installed in cars to track your location.

The TSA has moved way past airports, trains and sports stadiums, and is deploying mobile scanners to spy on people all over the place. This means that traveling within the United States is no longer a private affair.

You might also have seen the news this week that the Department of Homeland Security is going to *continue* to allow searches of laptops and phones based upon "hunches".

What's that about?

The ACLU published a map in 2006 showing that nearly two-thirds of the American public – 197.4 million people – live within a "constitution-free zone" within 100 miles of land and coastal borders:

The ACLU explained:

- Normally under the Fourth Amendment of the U.S. Constitution, the American people are not generally subject to random and arbitrary stops and searches.
- The border, however, has always been an exception. There, the longstanding view is that the normal rules do not apply. For example the authorities do not need a warrant or probable cause to conduct a “routine search.”
- But what is “the border”? According to the government, it is a 100-mile wide strip that wraps around the “external boundary” of the United States.
- As a result of this claimed authority, individuals who are far away from the border, American citizens traveling from one place in America to another, are being stopped and harassed in ways that our Constitution does not permit.
- Border Patrol has been setting up checkpoints inland — on highways in states such as California, Texas and Arizona, and at ferry terminals in Washington State. Typically, the agents ask drivers and passengers about their citizenship. Unfortunately, our courts so far have permitted these kinds of checkpoints – legally speaking, they are “administrative” stops that are permitted only for the specific purpose of protecting the nation’s borders. They cannot become general drug-search or other law enforcement efforts.

- However, these stops by Border Patrol agents are not remaining confined to that border security purpose. On the roads of California and elsewhere in the nation – places far removed from the actual border – agents are stopping, interrogating, and searching Americans on an everyday basis with absolutely no suspicion of wrongdoing.

- The bottom line is that the extraordinary authorities that the government possesses at the border are spilling into regular American streets.

Computer World reports:

> Border agents don't need probable cause and they don't need a stinking warrant since they don't need to prove any reasonable suspicion first. Nor, sadly, do two out of three people have First Amendment protection; it is as if DHS has voided those Constitutional amendments and protections they provide to nearly 200 million Americans.
>
> ***
>
> Don't be silly by thinking this means only if you are physically trying to cross the international border. As we saw when discussing the DEA using license plate readers and data-mining to track Americans movements, the U.S. "border" stretches out 100 miles beyond the true border. Godfather Politics added:
>
> > But wait, it gets even better! If you live anywhere in Connecticut, Delaware, Florida, Hawaii, Maine, Massachusetts, Michigan, New Hampshire, New Jersey or Rhode Island, DHS says the search zones encompass the entire state.
>
> Immigrations and Customs Enforcement (ICE) and Customs and Border Protection (CBP) have a "longstanding constitutional and statutory authority permitting suspicionless and warrantless searches of merchandise at the border and its functional equivalent." This applies to electronic devices, according to the recent CLCR "Border Searches of Electronic Devices" executive summary [PDF]:
>
> > Fourth Amendment
> >
> > The overall authority to conduct border searches without suspicion or warrant is clear and longstanding, and courts have not treated searches of electronic devices any differently than searches of other objects. We conclude that CBP's and ICE's current border search policies comply with the Fourth Amendment. We also conclude that imposing a requirement that officers have reasonable suspicion in order to conduct a border search of an electronic device would be operationally harmful without concomitant civil rights/civil liberties benefits. However, we do think that recording more information about why searches are performed would help managers and leadership supervise the use of border search authority, and this is what we recommended; CBP has agreed and has implemented this change beginning in FY2012.***

The ACLU said, Wait one darn minute! Hello, what happened to the Constitution? Where is the rest of CLCR report on the "policy of combing through and sometimes confiscating travelers' laptops, cell phones, and other electronic devices—even when there is no suspicion of wrongdoing?" DHS maintains it is not violating our constitutional rights, so the ACLU said:

> If it's true that our rights are safe and that DHS is doing all the things it needs to do to safeguard them, then why won't it show us the results of its assessment? And why would it be legitimate to keep a report about the impact of a policy on the public's rights hidden from the very public being affected?

***

As Christian Post wrote, "Your constitutional rights have been repealed in ten states. No, this isn't a joke. It is not exaggeration or hyperbole. If you are in ten states in the United States, your some of your rights guaranteed by the Bill of Rights have been made null and void."

The ACLU filed a Freedom of Information Act request for the entire DHS report about suspicionless and warrantless "border" searches of electronic devices. ACLU attorney Catherine Crump said "We hope to establish that the Department of Homeland Security can't simply assert that its practices are legitimate without showing us the evidence, and to make it clear that the government's own analyses of how our fundamental rights apply to new technologies should be openly accessible to the public for review and debate."

Meanwhile, the EFF has tips to protect yourself and your devices against border searches. If you think you know all about it, then you might try testing your knowledge with a defending privacy at the U.S. border quiz.

Wired pointed out in 2008 that the courts have routinely upheld such constitution-free zones:

> Federal agents at the border do not need any reason to search through travelers' laptops, cell phones or digital cameras for evidence of crimes, a federal appeals court ruled Monday, extending the government's power to look through belongings like suitcases at the border to electronics.
>
> ***
>
> The 9th U.S. Circuit Court of Appeals sided with the government, finding that the so-called border exception to the Fourth Amendment's prohibition on unreasonable searches applied not just to suitcases and papers, but also to electronics.
>
> ***
>
> Travelers should be aware that anything on their mobile devices can be searched by government agents, who may also seize the devices and keep them for weeks or months. When in doubt, think about whether online storage or encryption might be tools you should use to prevent the feds from rummaging through your journal, your company's confidential business plans or naked pictures of you and your-of-age partner in adult fun.

Going further down the high tech Big Brother rabbit hole, the FBI wants a backdoor to all software. The CIA wants to spy on you through your dishwasher and other appliances. Verizon has applied for a patent that would allow your television to track what you are doing, who you are with, what objects you're holding, and what type of mood you're in. (And some folks could conceivably be spying on you through your tv using existing technology.)

And they're probably bluffing and exaggerating, but the Department of Homeland Security claims they will soon be able to know your adrenaline level, what you ate for breakfast and what you're thinking ... from 164 feet away.

Indeed, technology has made pervasive spying more possible than ever before.

TechDirt notes:

> In a radio interview, Wall Street Journal reporter Julia Angwin (who's been one of the best at covering the surveillance state in the US) made a simple observation that puts much of this into context: the US surveillance regime has more data on the average American than the Stasi ever did on East Germans.

Postscript: This is not some "post-9/11 reality". Spying on Americans started before 9/11.

And the national security boys can choose to share U.S. civilian information with federal, state, local, or foreign entities for analysis of possible criminal behavior, even if there is no reason to suspect them.

And many say that the spying isn't being done to keep us safe ... but to crush dissent and to smear people who uncover unflattering this about the government ... and to help the too big to fail businesses compete against smaller businesses (and here).

And for other reasons. For example, the Atlantic notes:

> In 2008, NSA workers told ABC News that they routinely eavesdropped on phone sex between troops serving overseas and their loved ones in America.

Note: Here's a full report card on how well the government has been balancing civil liberties with other concerns.

Articles by: Washington's Blog