Written by **Joe Wolverton, II, J.D.** on September 26, 2013

The New Age of Surveillance

In an interview in June with a German television station, German President Joachim Gauck said the surveillance conducted by the National Security Agency (NSA) was not comparable to that conducted by the Stasi — the infamous East German Ministry for State Security — because "it is not like it was with the Stasi and the KGB — that there exist big filing cabinets in which all the content of our conversations are written down and nicely filed. This is not the case."

Gauck is right. The NSA is nothing like the Stasi because the East German secret police relied on such things as typewriters, carbon copies, handwritten transcriptions of phone conversations, agents listening through doors and rudimentary bugging devices, and the aforementioned filing cabinets. The NSA, on the other hand, can apparently monitor electronically — in real time — every word of every phone call, every text message, every social media post, every website visited, and every form of electronic communication.

How much data is being collected by the NSA? William Binney, a former NSA technical director turned whistleblower, estimates that the newly completed NSA Utah Data Center "will be able to handle and process five zettabytes of data." In a story quoting Binney's claim, National Public Radio reports that a zettabyte is equal to "the amount of data that would fill 250 billion DVDs."

Back to those bulging Stasi filing cabinets. Imagine that a typical filing cabinet with 60 files of 30 pages per file takes up about 4.3 square feet of space. Each 30-page file would equal roughly 120 MB of data. Given the amount of storage available to the NSA in its Utah location, if all the data stored there were printed and stored in traditional filing cabinets, those cabinets would occupy nearly 6.6 million square miles!

Nothing like the Stasi, indeed.

Secret Police Minus the Police Powers

Is there any clearer lens through which to view the future than the past? Is not the United States of 2013 eerily and tragically traveling along a similar trajectory to that followed by the formerly free Germans and the communist Stasi that ultimately deprived them of their liberties?

In describing the growth and survival of the East German surveillance state and the Stasi's activities that undergirded it, Scott Horton wrote that East Germany was a country "in which the power and authority of the intelligence services to spy on their own citizens rested on an elaborate network of laws that empowered surveillance and eroded the rights of citizens specified in the country's constitution."

Again, the Stasi and the Cold War communist East German regime had nothing on the NSA and 21st-century America.

From the enactment of the Patriot Act to the renewal of the Foreign Intelligence Surveillance Act amendments, Congress after Congress and consecutive presidents have usurped powers the scope of which are unknown in the written record of government.

Before launching into a report on the myriad methods being used by our own federal government to keep us under the constant vigilance of its never-blinking eye, the reader needs to have in the front of his mind the standard to which the federal government must be held.

The Fourth Amendment to the Constitution mandates:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Recent events demonstrate that for over a decade, our elected representatives (and the courts, for that matter) have disregarded the Constitution and built a domestic spy apparatus that bears no resemblance whatsoever to the blueprint provided by our Founding Fathers in the Constitution.

Throwing a Wrench Into the Works

On August 1, former low-level networking subcontractor Edward Snowden entered Russian territory.

Russian President Vladimir Putin permitted Snowden to take up temporary residence in Russia. At home, President Obama charged the young man with espionage, a curious charge given that even the president admits there is no evidence that Snowden transferred any sensitive information to a foreign government, an essential element of the crime he is accused of committing. No matter. President Obama is not known for hewing to the Constitution or the law.

The cache of documents Snowden holds was leaked to the *Washington Post* and to *The Guardian* (U.K.) and contains compelling evidence of the NSA's wholesale violation of the Fourth Amendment through the dragnet surveillance of phone records and monitoring of Internet traffic.

With the assistance of Glen Greenwald of *The Guardian*, Snowden has leaked one constitutional violation after another committed by the NSA. All of which, it must be understood, was done with the cooperation of the president, the Congress, and the courts. The strength of the evidence of collusion among the three branches of the federal government in the de facto repeal of the Fourth Amendment is overwhelming.

Tyranny Erected in Cyberspace

Among the most disturbing disclosures found within the reams of Edward Snowden's revelations was the surrender by major telecommunications companies of the otherwise private phone records of millions of Americans — none of whom was, as required by the Constitution, suspected of committing any sort of crime.

According to a court order labeled "TOP SECRET," federal judge Roger Vinson ordered Verizon to turn over the phone records of millions of its U.S. customers to the NSA.

The order, issued in April by the U.S. Foreign Intelligence Surveillance Court and leaked on the Internet by *The Guardian*, compels Verizon to provide these records on an "ongoing daily basis" and to hand over to the domestic spy agency "an electronic copy" of "all call detail records created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."

This information includes the phone numbers involved, the electronic identity of the device, the calling card numbers (if any) used in making the calls, and the time and duration of the call.

In other words, millions of innocent Americans have had their call records shared with a federal spy agency in open and hostile defiance of the Fourth Amendment's guarantee of the right of the people to be free from such unreasonable searches and seizures.

What is reasonable? Legally speaking, "the term reasonable is a generic and relative one and applies to that which is appropriate for a particular situation."

Even if the reasonableness threshold is crossed, though, there must be a warrant and suspicion of commission of or intent to commit a crime. Neither the NSA nor Verizon has asserted that even one of the millions whose phone records were seized fits that description.

When contacted by *The New American*, a spokesman for Verizon declined to comment on his company's compliance with the order.

Such a demur is expected in light of the provision of the order that prohibits Verizon, the FBI, or the NSA from revealing to the public — including the Verizon customers whose phone records now belong to the Obama administration — that the data is being given to the government.

Glen Greenwald of *The Guardian* details the data being seized by the NSA:

> The information is classed as "metadata," or transactional information, rather than communications, and so does not require individual warrants to access. The document also specifies that such "metadata" is not limited to the aforementioned items. A 2005 court ruling judged that cell site location data — the nearest cell tower a phone was connected to — was also transactional data, and so could potentially fall under the scope of the order.

While the order itself does not include either the contents of messages or the personal information of the subscriber of any particular cell number, its collection would allow the NSA to build easily a comprehensive picture of who any individual contacted, how and when, and possibly from where, retrospectively.

Perhaps the most disturbing take-away from the leak of this secret court document ordering Verizon to hand over customer call logs and other data to a federal surveillance agency is the fact that the government considers the protections of the Fourth Amendment to be nothing more than a "parchment barrier" that is easily torn through. The Obama administration regards the Constitution — as did the Bush administration before it — as advisory at best.

Of course, being a subcontractor in the construction of the surveillance state pays handsomely. As reported by *The New American*, on August 16, Verizon announced that it was awarded a 10-year, $10-billion contract "to provide cloud and hosting services" to the U.S. Department of the Interior.

Apparently, crimes against the Constitution pay, and they pay very well.

Social Media Surveillance

Have you updated your Facebook or Twitter accounts lately? If so, the government likely knows what you posted, when you posted it, and who read what you wrote.

According to a statement posted on Facebook's website June 14, government agencies — including federal, state, and local authorities — requested user data on between 18,000 and 19,000 account holders.

The remarkable disclosure of government requests for users' private information follows successful negotiations between Facebook and other tech giants and the federal government.

Over the past few weeks, Facebook, Google, and other technology companies who were implicated in the revelations of the covert NSA surveillance program known as PRISM have petitioned the feds to allow them to disclose their level of participation in surveillance requests received from government entities.

Under PRISM, the NSA and the FBI are "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person's movements and contacts over time," as reported by the *Washington Post*.

One document in the Snowden revelations indicated that PRISM was "the number one source of raw intelligence used for NSA analytic reports." Snowden claimed that the program was so invasive that the NSA and the FBI "quite literally can watch your ideas form as you type."

Most of these requests by the government are made under the authority of the Foreign Intelligence Surveillance Act (FISA). Not surprisingly, when the government asks the special surveillance court to approve their snooping, judges give them the go-ahead.

In fact, in April, the Department of Justice revealed to Congress the number of applications for eavesdropping received and rejected by the FISA court: In 2012, of the 1,789 requests made by the government to monitor the electronic communications of citizens, not a single one was rejected.

Following the negotiations that opened the way for Facebook to report its cooperation with requests to hand over user information, Microsoft made a similar surveillance disclosure. A blog post on the Redmond, Washington-based company's website declared:

> For the six months ended December 31, 2012, Microsoft received between 6,000 and 7,000 criminal and national security warrants, subpoenas and orders affecting between 31,000 and 32,000 consumer accounts from U.S. governmental entities (including local, state and federal).

According to the information Snowden released, both companies that disclosed government surveillance requests — Facebook and Microsoft — were giving the government access to the private information of millions of users.

They were not alone, however. Yahoo, Google, PalTalk, AOL, Skype, YouTube, and Apple all allowed the agents of the federal surveillance state to secretly snoop on their users.

Every Keystroke Recorded

On July 31 Glen Greenwald published another drip in the ocean of Snowden leaks. Under a program known as "XKeyscore," the NSA monitors and records every e-mail written by every American, again without a warrant and without probable cause, in direct defiance of the Fourth Amendment.

Greenwald, after examining a PowerPoint presentation included in the information he received from Snowden, explained the scope of XKeyscore: "One presentation claims the [XKeyscore] program covers 'nearly everything a typical user does on the internet,' including the content of emails, websites visited and searches, as well as their metadata." "Analysts can also use XKeyscore and other NSA systems to obtain ongoing 'real-time' interception of an individual's internet activity," he added.

How does it work? Greenwald explained that, too: "An NSA tool called DNI Presenter, used to read the content of stored emails, also enables an analyst using XKeyscore to read the content of Facebook chats or private messages. Analysts can also search by name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used."

It is important to note that XKeyscore doesn't record phone conversations. There is evidence, however, that the NSA records every one of those, as well, and stores the content in one of its many data warehouses, such as the one in Utah that goes online within weeks.

Of course, there is no doubt that mobile phone conversations are being recorded.

The federal government is remotely activating the microphones and cameras in Android smartphones and Windows laptops, according to a report published by the *Wall Street Journal* on August 3.

Citing a "former US official," the *Journal* says court documents reveal that the FBI is using a variety of "hacking" tools to ramp up the scope of the surveillance of millions of Americans, keeping many unwittingly under the watchful eye of Washington.

One of the *Journal's* anonymous sources described a part of the FBI called the "Remote Operations Unit." Agents in this specialized unit prefer, if possible, to install the remote control software by uploading to the target's computer using a USB flash drive. When the g-men-come-hackers can't get access to the target's computer, they install the surveillance software over the Internet "using a document or link that loads software when the person clicks or views it."

It is not only possible for the federal government to listen to your conversations using the microphone in your Android smartphone and watch you while you sit in your own home on your own computer, but they do so regularly and can do so very easily.

Purportedly, the FBI has been using these methods of surveillance "for over a decade," but their use has come to light only recently by way of "court documents and interviews" with people familiar with the programs.

Is the NSA Policing Itself?

In what likely amounts to another middling misdirection, on August 15 the *Washington Post* reported that an internal audit of the NSA revealed that the agency violated its own privacy protection rules 2,776 times.

NSA Compliance Director John DeLong tried putting a positive spin on the report. During a press conference on August 16, DeLong assured the media that the NSA is not involved in "willful violations" of the law.

"People need to understand there's no willful violations here," he said. "We really do look for them, detect them and correct them." "No one at NSA, not me or anyone else, thinks they are okay," he added.

He additionally claimed that the number of incidental violations of privacy laws is "minuscule … a couple over the past decade."

Minuscule or not, why is such a disclosure irrelevant? Consider the following analysis published by Ron Paul on his Ron Paul Institute for Peace and Prosperity website:

> Though it made for sensational headlines last week, the 2,776 NSA violations of its own intercept guidelines over the course of one year are irrelevant. The millions and millions of "authorized" intercepts of our communications are all illegal — except for the very few carried out in pursuit of a validly-issued search warrant in accordance with the Fourth Amendment. That is the real story. Drawing our attention to the violations unfortunately sends the message that the "authorized" spying on us is nothing to be concerned about.

E-mail and Snail Mail

The U.S. government is not content to monitor your phone calls and your Internet activity; it's now reading your snail mail, too.

A story in the *New York Times* published Wednesday, July 3, tells the story of Buffalo, New York, resident Leslie James Pickering. Pickering reports that last September he noticed "something odd in his mail": a "handwritten card, apparently delivered by mistake, with instructions for postal workers to pay special attention to the letters and packages sent to his home," the *Times* story claims.

The card — a picture of which appears in the *Times* story — appears to read: "Show all mail to supv [supervisor] for copying prior to going out on the street." Pickering's name was written on the card, as well as the word "Confidential," written in green ink. Apparently, Pickering was the unwitting target of a "longtime surveillance system" the *Times* calls "mail covers."

It doesn't stop there, however. While snail mail surveillance has been a tool of law enforcement for over a century, the program that targeted Pickering is called Mail Isolation Control and Tracking. As part of this surveillance tactic, the "Postal Service computers photograph the exterior of every piece of paper mail that is processed in the United States — about 160 billion pieces last year. It is not known how long the government saves the images."

When combined, the NSA and the U.S. Postal Service can keep every form of communication — electronic and conventional — under constant surveillance, without probable cause.

All Movements Are Monitored

Beyond the government's ability to watch and record every activity carried on in cyberspace, its capacity for keeping an eye on the real world comings and goings of citizens is immensely more jarring and less publicized.

The U.S. government exercises control over a massive and technologically advanced camera-based surveillance system that has the capacity to keep the urban population of this country under the watchful eye of government 24 hours a day.

TrapWire is the name of this network of cameras and other surveillance tools. Unlike other elements of the central government's cybersurveillance program, word about TrapWire was not leaked by Obama administration insiders. The details of this nearly unbelievable surveillance scheme were made public by WikiLeaks, the anti-secrecy group founded by Julian Assange.

Exactly what is TrapWire? According to one description of the program, from the online Russia Today:

> Former senior intelligence officials have created a detailed surveillance system more accurate than modern facial recognition technology — and have installed it across the US under the radar of most Americans, according to emails hacked by Anonymous.

Every few seconds, data picked up at surveillance points in major cities and landmarks across the United States are recorded digitally on the spot, then encrypted and instantaneously delivered to a fortified central database center at an undisclosed location to be aggregated with other intelligence.

As with so many of the federal government's unconstitutional efforts at placing each and every citizen of the United States under the never-blinking eye of those who consider themselves our caretakers, TrapWire is sold as being a necessary weapon in the War on Terror.

Taxes as a Political Tool

Other departments in the executive branch have done as much to keep an eye on potential enemies of the state as the NSA, albeit in their own distinct manner.

Earlier this summer, it was reported by many outlets (including *The New American*) that the IRS was persecuting Tea Party and other conservative groups by conducting intrusive and illegal investigations of these groups' applications for 501(c)(4) tax-exempt status.

Although according to the White House the discrimination ended in May 2012, on August 9, 2013, the *Washington Examiner* reported that an unnamed IRS official testified in a closed-door hearing of the House Ways and Means Committee that "the agency is still targeting Tea Party groups."

The implications of this abuse are incalculable. In a statement to *The New American*, Senator Rand Paul (R-Ky.) said, "The power to audit has become a political weapon. Nobody wants a government where the taxing authority is used politically."

The use of taxing authority as a political weapon was not confined to conflicts with non-profit petitions.

In January, Christine O'Donnell, former candidate for Joe Biden's former Senate seat in Delaware, was informed that Delaware state officials had on several occasions accessed her federal tax records to obtain potentially embarrassing information on a tax lien that was first reported in a newspaper article.

The lien, it was discovered, was erroneously filed, and the snooping was discovered.

During congressional hearings on the matter and on IRS corruption in general, a spokesman for the IRS told Senator Chuck Grassley (R-Iowa) that a Delaware state investigator was given permission to open O'Donnell's IRS records.

Based on nothing more than a newspaper story, O'Donnell's political foes were able to gain access to her very private tax information. Most Americans, it would seem, would prefer that the information contained in their IRS file would remain private. The fact is, however, if an agent of the government (state or federal) wants to rifle through that file, the IRS requires very little in the way of probable cause of wrongdoing. Being a member of a group whose politics don't jibe with the establishment is apparently sufficient grounds for this very invasive, illegal, and unconstitutional surveillance.

Despite the government's intrusions into Americans' private business, many Americans dismiss its activities, saying, "I've done nothing wrong. Why should I worry?" This is the question often put to opponents of the federal government's surveillance activity. Furthermore, many Americans accept the surveillance state with rationalizations such as: "The government is protecting us from terrorism, so I think it's fine that they keep an eye out for extremists. If they happen to listen to my phone calls or read my e-mail, that's just the price we pay for safety."

In light of the protections afforded by the Fourth Amendment, these mentalities look at the surveillance from the wrong angle.

Americans are endowed by their Creator with the right to be free from unwarranted searches and seizures. When the government takes away these rights, then there is no liberty, regardless of pretexts and purposes put forth by the federal government.

While it's true that most Americans have "done nothing wrong" criminally speaking, it is equally true that most of us have done many embarrassing things that we would prefer not to have put in a file for future use by political enemies — inside or outside the government. What are these possible peccadilloes? Think bad credit, poor scholastic performance, Web surfing habits, sensitive medical diagnoses, etc.

It is most important to remember that there is no evidence that the government's massive surveillance and deprivations of rights has made us any safer. What, then, is the true purpose of the surveillance?

It isn't security. Demanding freedom in exchange for safety is the economy of tyrants. When the federal government — or any government — robs citizens of their basic civil rights, then that government has become despotic by definition.

Benjamin Franklin said, "Any society that would give up a little liberty to gain a little security will deserve neither and lose both." President Obama, on the other hand, told Americans that we cannot have a nation that is 100 percent safe and 100 percent private. To be safe, he says, we have to make hard choices.

He's right: We must choose whether to allow our constitutional rights to be subjected to daily diminution or to stand up and demand that the totalitarianism end and liberty be restored. The question is: How?

Federalism Protects Fundamental Freedom

One unwarranted wiretap, one unwarranted seizure of a phone record, one search of records of an individual's digital communications is too many. If we are a Republic of laws, then the supreme constitutional law of the land must be adhered to. The standard is not whether or not the spies or their bosses think the deprivations are "okay." The standard is the Constitution — for every issue, on every occasion, with no exceptions. Anything less than that is a step toward tyranny.

Taken together, the roster of snooping programs in use by the federal government places every American under the threat of constant surveillance. The courts, Congress, and the president have formed an unholy alliance bent on obliterating the Constitution and establishing a country where every citizen is a suspect and is perpetually under the never-blinking eye of the government.

The establishment will likely continue construction of the surveillance until the entire country is being watched around the clock and every monitored activity is recorded and made retrievable by agents who will have a dossier on every American.

The fight can yet be won, though. Americans can attack the sprawling surveillance state on several fronts. First, we must elect men and women to federal office who will honor their oaths of office to preserve, protect, and defend the Constitution. Then, once in office, each of them must be held immediately accountable for each and every violation of that oath.

Next, we must fill our state legislatures with men and women who will refuse to enforce any act of the federal government that exceeds the boundaries of its constitutionally granted powers. These lawmakers must force the federal beast back inside its constitutional cage and never accept even a degree of deviation from the blueprint drawn in Philadelphia in 1787.

Though the hour is late, there is still hope. Beginning today, Americans can refuse to re-elect any lawmaker who has voted to fund the NSA or any other federal agency whose existence is not specifically permitted by the Constitution. We can unite, as our forefathers, in the ennobling cause of the end of tyranny and the promotion of those unalienable rights granted to us — and revocable only — by our Creator.

profiles, immigration, healthcare, foreign policy, guns, etc. Digital as well as print options are available!