
My blog: War Department/Peace Department
http://jamesrichardbennett.blogspot.com/

My Newsletters:
http://www.omnicenter.org/newsletter-archive/

For an informed and resistant citizenry. See: Bush, CIA, FBI, Drones, National Security State, NSA, Top Secret, Intelligence Industry Complex, Imperialism, Fascism, Obama, Snowden, Greenwald, and more.

Index:
http://www.omnicenter.org/omni-newsletter-general-index/

Visit OMNI’s Library.

"I refuse to live in a country like this, and I'm not leaving"
Michael Moore

From the White House: Write or Call
President Obama is committed to creating the most open and accessible administration in American history. That begins with taking comments and questions from you, the public, through our website.

Call the President

PHONE NUMBERS
Comments: 202-456-1111
Switchboard: 202-456-1414

TTY/TTD
Comments: 202-456-6213
Visitor's Office: 202-456-2121

Write a letter to the President

Here are a few simple things you can do to make sure your message gets to the White House as quickly as possible.

1. If possible, email us! This is the fastest way to get your message to President Obama.
2. If you write a letter, please consider typing it on an 8 1/2 by 11 inch sheet of paper. If you hand-write your letter, please consider using pen and writing as neatly as possible.

3. Please include your return address on your letter as well as your envelope. If you have an email address, please consider including that as well.

4. And finally, be sure to include the full address of the White House to make sure your message gets to us as quickly and directly as possible:

   **The White House**
   1600 Pennsylvania Avenue NW
   Washington, DC 20500

Nos. 3, 4, 5, 6 at end

**Contents #7  Sept. 11, 2013**

Resisting National Security Abuse
Free Press Action Fund
Free Press.net
Rothschild, US NSS
Durst, US NSS: NSA
Webb, US/UK Surveillance/Assassination Police States
NSA vs. Fourth Amendment
VFP, Feds Caught in Lies
VFP, FBI Tapping Phones
Jay Rosen, NSA Controlling Johns Hopkins
Greenwald, et al., NSA Intelligence to Israel

**Contents #8, Oct. 18, 2013**

DC Stop Watching Us Rally October 26
Greenwald, End of Privacy
NSA Chief Admits Full Collection of GPS Cell Phone Data
NSA Reporting in the *Arkansas Democrat-Gazette*
Calabrese and Harwood: US National Surveillance State
Noam Chomsky
Risen and Poitras in *NYT*, NSA Spies on Social Relations
Tech leaders urge Obama to move on NSA overhaul

Alistair Barr and Aamer Madhani, USA TODAY 4:18 p.m. EST December 17, 2013
WASHINGTON — Tech executives urged President Obama on Tuesday to "move aggressively" to overhaul the way the U.S. government conducts surveillance.

The push came during a private meeting with Obama at the White House, which was billed as an opportunity to brief industry leaders on the progress the administration has made solving problems with the federal online health care exchange as well as the fallout that national security leaks have had on their companies.

Among those at the White House meeting were Apple's CEO Tim Cook, Yahoo! CEO Marissa Mayer, Facebook Chief Operating Officer Sheryl Sandberg and Google's executive chairman, Eric Schmidt.

A federal judge ruled Monday that the National Security Agency's controversial surveillance program that collects millions of Americans' telephone records may be unconstitutional. On Tuesday, White House press secretary Jay Carney said the administration believes the surveillance program is constitutional.
Officials from eight companies — including AOL, Apple, Facebook and Google — wrote an open letter to Obama and Congress last week in which they plainly stated their call to curb surveillance.

Among the changes the group requests of government: to codify limitations on its ability to compel service providers to disclose user data; to bolster oversight of intelligence agencies collecting information; and to allow companies to publish the number of instances and nature of government demands for user information.

"We appreciated the opportunity to share directly with the president our principles on government surveillance that we released last week and we urge him to move aggressively on reform," the executives said in a joint statement.

Schmidt, of Google, opened the meeting and laid out industry officials' concerns. Obama seemed sympathetic to the idea of allowing more disclosure of government surveillance requests by technology companies, according to a tech industry official who was briefed on the meeting. The official asked to remain anonymous because the meeting was private.

Mayer, the Yahoo! executive, brought up concerns about the potentially negative impact that could be caused if countries, such as Brazil, move forward with legislation that would require service providers to ensure that data belonging to a citizen of a certain country remain in the country it originates, the official said.

That would require technology companies to build data centers in each country — a costly problem for American Internet companies, the official said. The White House noted in a statement after the meeting that the group discussed the "economic impacts of unauthorized intelligence disclosures."

The White House announced Friday that Obama received 40 recommendations from a special study group he tasked with reviewing the U.S. intelligence community's collection of telephone and Internet data. The study group was created in the aftermath of revelations made by former National Security Agency contractor Edward Snowden.

Obama's action on the recommendations — which he is weighing and expected to announce next month — are of significant importance to companies such as Google, Facebook, Apple and others who are dealing with the fallout of reports based on Snowden's leaks that the NSA gained access to some of their users' information.

In a light moment at the start of the meeting, Obama asked Netflix CEO Reed Hastings about whether he brought any advance copies of the second season of the soon-to-be-released House of Cards. Obama joked about his admiration for the Netflix-produced program, which is based in Washington and features a power-hungry politician played by actor Kevin Spacey.

"I wish things were that ruthlessly efficient," Obama said. The president added about Spacey's
Reform Government Surveillance

The undersigned companies believe that it is time for the world’s governments to address the practices and laws regulating government surveillance of individuals and access to their information.

While the undersigned companies understand that governments need to take action to protect their citizens’ safety and security, we strongly believe that current laws and practices need to be reformed.

Consistent with established global norms of free expression and privacy and with the goals of ensuring that government law enforcement and intelligence efforts are rule-bound, narrowly tailored, transparent, and subject to oversight, we hereby call on governments to endorse the following principles and enact reforms that would put these principles into action.

Global Government Surveillance Reform
The Principles

1. Limiting Governments’ Authority to Collect Users’ Information

Governments should codify sensible limitations on their ability to compel service providers to disclose user data that balance their need for the data in limited circumstances, users’ reasonable privacy interests, and the impact on trust in the Internet. In addition, governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications.

2. 


Intelligence agencies seeking to collect or compel the production of information should do so under a clear legal framework in which executive powers are subject to strong checks and balances. Reviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner so that the courts are accountable to an informed citizenry.

3. Transparency About Government Demands
Transparency is essential to a debate over governments’ surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly disclose this data publicly.

4. Respecting the Free Flow of Information
The ability of data to flow or be accessed across borders is essential to a robust 21st century global economy. Governments should permit the transfer of data and should not inhibit access by companies or individuals to lawfully available information that is stored outside of the country. Governments should not require service providers to locate infrastructure within a country’s borders or operate locally.

5. Avoiding Conflicts Among Governments
In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved mutual legal assistance treaty — or “MLAT” — processes. Where the laws of one jurisdiction conflict with the laws of another, it is incumbent upon governments to work together to resolve the conflict.

Voices For Reform

“AOL is committed to preserving the privacy of our customers’ information, while respecting the right of governments to request information on specific users for lawful purposes. AOL is proud to unite with other leading Internet companies to advocate on behalf of our consumers.” —Tim Armstrong, Chairman and CEO, AOL

“Reports about government surveillance have shown there is a real need for greater disclosure and
new limits on how governments collect information. The US government should take this opportunity to lead this reform effort and make things right.”—Mark Zuckerberg, CEO, Facebook

“The security of users’ data is critical, which is why we’ve invested so much in encryption and fight for transparency around government requests for information. This is undermined by the apparent wholesale collection of data, in secret and without independent oversight, by many governments around the world. It’s time for reform and we urge the US government to lead the way.”—Larry Page, CEO, Google

“These principles embody LinkedIn’s fundamental commitment to transparency and ensuring appropriate government practices that are respectful of our members’ expectations.”—Erika Rottenberg, General Counsel, LinkedIn

“People won’t use technology they don’t trust. Governments have put this trust at risk, and governments need to help restore it.”—Brad Smith, General Counsel and Executive Vice President, Legal and Corporate Affairs, Microsoft

“Twitter is committed to defending and protecting the voice of our users. Unchecked, undisclosed government surveillance inhibits the free flow of information and restricts their voice. The principles we advance today would reform the current system to appropriately balance the needs of security and privacy while safeguarding the essential human right of free expression.”—Dick Costolo, CEO, Twitter

“Protecting the privacy of our users is incredibly important to Yahoo. Recent revelations about government surveillance activities have shaken the trust of our users, and it is time for the United States government to act to restore the confidence of citizens around the world. Today we join our colleagues in the tech industry calling on the United States Congress to change surveillance laws in order to ensure transparency and accountability for government actions.”—Marissa Mayer, CEO, Yahoo

An open letter to Washington

Dear Mr. President and Members of Congress,

We understand that governments have a duty to protect their citizens. But this summer’s revelations highlighted the urgent need to reform government surveillance practices worldwide. The balance in many countries has tipped too far in favor of the state and away from the rights of the individual — rights that are enshrined in our Constitution. This undermines the freedoms we all cherish. It’s time for a change.

For our part, we are focused on keeping users’ data secure — deploying the latest encryption technology to prevent unauthorized surveillance on our networks and by pushing back on government requests to ensure that they are legal and reasonable in scope.

We urge the US to take the lead and make reforms that ensure that government surveillance efforts are clearly restricted by law, proportionate to the risks, transparent and subject to independent oversight. To
see the full set of principles we support, visit ReformGovernmentSurveillance.com

Sincerely,

AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo

Jim Sensenbrenner, The NSA Overreach Poses a Serious Threat to Our Economy


Sensenbrenner writes: "The overreach by the National Security Agency (NSA) does more than infringe on American civil liberties. It poses a serious threat to our economic vitality."
Tell Congress to Support the USA Freedom Act.

Dear Dick,

Rep. Jim Sensenbrenner and Sen. Patrick Leahy just introduced the USA Freedom Act, which would end the NSA's bulk collection of our phone records and require more oversight and transparency of the agency's domestic surveillance programs.¹

Tell Your Members of Congress to Support the USA Freedom Act.

Even Sensenbrenner — one of the Patriot Act's authors — thinks the NSA has gone too far. This bipartisan bill would prevent the NSA from spying on all of us — limiting the agency to collecting data on actual targets of criminal investigations. And it would mean the end of the NSA's “back-door” warrantless searches of Americans' private information.

Tell Congress to Protect Our Privacy and Pass the USA Freedom Act.

The momentum has shifted in our direction. Thousands of people attended Saturday's Rally Against Mass Surveillance,² foreign heads of state have expressed outrage over NSA spying — and your emails, phone calls, social-media shares and chats by the watercooler have changed the conversation about government surveillance.

The NSA's programs — coupled with decades of attacks on the privacy rights of immigrants, communities of color and Muslim Americans — mean that we're all living in a culture of surveillance.

Local and federal agencies track our phone calls and mine our Internet use. They use race and religion to target entire communities and track millions of innocent people. And they won't stop until people from across the country and across the political spectrum unite in opposition.

The USA Freedom Act will go a long way toward restoring our Fourth Amendment rights to connect and communicate in private. At a moment when journalists are under attack like never before and the open Internet is in peril, we need to make sure Congress comes out in support of this bill.

Urge Your Members of Congress to End the Surveillance. Tell Them to Support the USA Freedom Act.

Making change on this front will take years — but passing this bill is the first step.

Thanks for all that you do,

Josh, Matt, Candace and the rest of the Free Press Action Fund team

P.S. The Free Press Action Fund fights every day to protect your privacy. We don’t take money
from business, government or political parties and rely on the generosity of people like you to fuel our work. **Please donate $15 (or more!) today. Thank you!**


2. "Rally Against Mass Surveillance," [rally.stopwatching.us](http://rally.stopwatching.us)
   The Free Press Action Fund is a nonpartisan organization building a nationwide movement for media that serve the public interest. The Free Press Action Fund does not support or oppose any candidate for public office. Learn more at [www.freepress.net](http://www.freepress.net).
   Join us on [Facebook](http://Facebook) and follow us on [Twitter](http://Twitter).

31 October 13 AM, **Reader Supported News**

**Snowden Files: Google and Yahoo Furious Over NSA Intercept Report**
*Dominic Rushe, Spencer Ackerman and James Ball, Guardian UK*

Rushe, Ackerman, and Ball report: "Google and Yahoo, two of the world's biggest tech companies, reacted angrily to a report on Wednesday that the National Security Agency has secretly intercepted the main communication links that carry their users' data around the world."

[READ MORE](http://READ MORE)

---

Secretary of State Kerry: Reinstate Edward Snowden’s
Thank you for asking the Secretary of State to reinstate Edward Snowden's passport. Please support this campaign by donating here. Please take a few moments to post on Facebook and Tweet it out, and email your friends with the form below.

Send mail from your own address book

Illustration by Rachel K Dooley

FEATURES » OCTOBER 17, 2013

Return to Nixonland
How the NSA slipped its leash under Bush and Obama.

BY LISA GRAVES

Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about
us, the more power it has over us.

The documents leaked by Edward Snowden and published by the Guardian and other outlets confirm what privacy advocates have been saying for years: The government has secretly turned its most powerful weapons of foreign intelligence surveillance inward on millions of Americans.

How can an ordinary citizen cut through the brush—with the avalanche of complicated, classified materials released, the flurry of political finger-pointing, and the various denials and narrowly crafted dodges? Welcome to a guided tour of the National Security Agency (NSA) scandal. We’ll explore how we got here and what Nixon’s got to do with it.

Who? Me?

The NSA has rebuffed demands by some in Congress for an estimate of the number of Americans whose information has been gathered, stored and searched, but the math is simple. Unless you are a child, a Luddite or a hermit who has never dialed a phone or used the Internet, records of your phone calls and online interactions have been captured by the NSA.

This includes your number and everyone you dial or text, plus how of- ten and how long you talk, as well as your location—although the NSA has claimed it doesn’t actually use the location data. In other words, the NSA has the fact of all your calls with your friends, family, lover(s), bank(s) and doctors’ offices for whatever ails you, along with calls to psychic hotlines or phone sex workers, if that’s your thing. The number of innocent Americans affected: at least 260 million.

That’s not all. For nearly a decade, the NSA was gathering records about Americans’ “Internet transactions,” including “metadata” such as the “to, from, cc and bcc lines of a standard email,” when your email was sent and opened, your IP address and location, and an array of data about you as you search the Internet, and interact with friends and strangers through social media. That program is no longer authorized by a secret court in Washington, D.C., but whether it continues is unknown. Also unknown: whether the NSA’s gathering of Americans’ credit card transactions is continuing or was secretly stopped.

Even that’s not all. Though the NSA has emphasized that it does not obtain the “contents” of your calls or emails through this program, the government has decided that the contents of all international phone calls and emails “to or from” Americans and others abroad are fair game for acquisition by the NSA without a warrant. At least 40 million American citizens travel internationally each year, and America is home to 40 million immigrants, who call or email their loved ones overseas about their most intimate worries and desires.

And there’s more. Newly declassified documents prove that countless purely “domestic” conversations between innocent Americans here in the United States have also been acquired and searched by the NSA.

Additionally, the affidavits in lawsuits filed in 2006 by the Electronic Frontier Foundation present evidence that shortly after 9/11 the NSA installed “NARUS” devices at AT&T’s main transmission station in San Francisco and at other telecommunications hubs across the
country. Those devices are designed to make a duplicate of the communications stream (content and data) as it passes through the system at the speed of light.

Accordingly, such devices can give the NSA access to all American domestic and international phone calls and Internet activity that travel through AT&T, which provides the backbone of the communications system that other phone and Internet service providers rely on. So, as a technological matter, if law were no barrier, the evidence indicates that the NSA could technically acquire, store and analyze almost every word spoken or written on American phones and computers.

Snowden’s revelations include Power Point presentations referencing an array of tools—with code names like “PRISM”—the NSA has used to target the social media activities, Internet searches and emails of specific people. But there’s still a lot we don’t know. And that’s a problem in a democracy in which the government is supposed to govern by consent of the people.

The risk of ‘total tyranny’

Sen. Frank Church (D-Idaho) said after his investigation of the NSA in 1975, following leaks about President Richard M. Nixon’s use of the NSA to spy on his enemies, opponents of the war in Vietnam and others:

If this government ever became a tyrant, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology. ... We must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision so that we never cross over that abyss. That is the abyss from which there is no return.

Those were the late Senator Church’s fears before almost every American had a “smart phone” and before most of us heard of the Internet—which in the 1970s was merely a computer network within the Pentagon and a few Silicon Valley companies—let alone traversed it daily.

Indeed, before Google was a word, let alone an empire; before almost all of our telephone conversations, emails and transactions of daily life were transmuted into a searchable digital world; and before a handful of murderers crashed into the World Trade Center and the Pentagon on September 11, 2001, we needed greater protections for our privacy and liberty. Now that need is even more urgent.

Along with the seismic transformation in the way we communicate, the legal controls on the NSA’s powers have been systematically loosened, if not obliterated, by the White House, Congress and the courts at the urging of leaders of the military intelligence community.

The NSA says it has “internal controls” but once information about Americans is stored by the NSA—including in a gargantuan 1-million-square-foot data storehouse being finalized in Bluffdale, Utah—it can be accessed by numerous civilians at home and abroad. The agency claims there have been only 12 incidents of NSA staffers using its “Signals Intelligence” (SIGINT) improperly. Most of them spied on lovers, such as girlfriends suspected of infidelity. However, almost all of these were discovered only through polygraph tests of workers
renewing security clearances. How many more times have lovers or enemies been “targeted” by government employees, the military and intelligence contractors with access to the trove of SIGINT data?

More importantly, how can we ever trust that the NSA’s new powers won’t be misused by those in power? We already know that during the Occupy Wall Street protests, federal “counterterrorism” dollars were used by the Federal Bureau of Investigation, the Department of Homeland Security and local law enforcement to monitor Americans guilty only of speaking against Wall Street’s destruction of our economy and its corruption of our democracy. And the government got away with it.

So the question isn’t whether the information that the NSA has been allowed to gather on Americans will be misused. The question is, when? And by whom? Perhaps our next president? Religious- Reactionary Rick (Santorum)? Tea Party Ted (Cruz)? Take-Two Rick (Perry)? You may laugh, but remember that prior to the 1980 presidential election, Trees-Cause-More-Pollution-Than-Automobiles Ronald (Reagan) was a joke.

Who in the NSA’s quasi-military hierarchy has the power to question a demand to provide information in its databases about specific Americans when made under the authority of the commander in chief, no matter who the president is or which power-hungry advisors aid the White House in 2016 or 2020 or beyond?

It’s a state of affairs that would make Nixon smirk. It’s also why foreign citizens who’ve lived under authoritarian regimes, in Germany and elsewhere, have expressed some of the greatest horror at the revelations over the NSA’s ubiquitous monitoring.

**The past isn’t even past**

To understand what happened to the rule of law since 9/11, it’s important to understand the path of the law before the World Trade Center towers fell.

It begins with the Fourth Amendment, which makes no distinction between “intelligence gathering” and “law enforcement.” The Constitution speaks instead to the rights of Americans regardless of the agent that would violate them:

> 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.

Those words were born of the vanquishing of an authoritarian tyrant whose officers used “general warrants” to search colonists at will to protect the crown and its interests.

Surprisingly, it was not until 1967 that the Supreme Court ruled that the government needed a warrant to listen to Americans’ phone calls. The following year, in 1968, Congress passed a crime bill to provide rules for obtaining warrants for wiretaps but—at the secret urging of the NSA—the legislature exempted surveillance in the name of national security.

In November of that year, Nixon was elected president.

In 1969, just six months after taking office, Nixon directed the NSA to search its files for information on specific Americans whom he and J. Edgar Hoover had placed on a watch list.
At that time, the existence of the NSA, formally established in 1952, was so secret that almost no one in Congress knew about it, and its funding was concealed in the Pentagon’s classified “black budget.” For decades, the NSA and its predecessors had acted as the government’s signal corps, listening for radio communications from enemy ships, tapping into the cables of diplomats of the Soviet Union and decrypting ciphers sent by spies. Unbeknownst to Congress, the NSA and its predecessor, the Armed Forces Security Agency, had also been spying on Americans for decades, making duplicates of all of the international telegrams sent to or from Americans by “wire” or cable since 1945, as well as gathering radio transmissions from across the globe through earth-bound satellite receivers and satellites. By the early 1970s, the NSA’s analysts were reading over 150,000 telegrams to or from Americans a month under that program, called “Operation SHAMROCK.”

With this vast and secret intelligence-gathering apparatus at his disposal, Nixon later expanded his watch list, directing the NSA to search for anything “subversive” or related to drug-dealing. In the meantime, in 1972, a case involving Nixon spying on Americans under the guise of national security, with no link to a foreign government, made its way to the Supreme Court. In that case, known as the Keith case, the Court unanimously declared:

The Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. ... The Fourth Amendment does not contemplate the executive officers of Government as neutral and disintersted magistrates.

In August 1974, in the wake of the Watergate scandal involving the illegal surveillance activities of the Committee to Re-Elect the President (CREEP), Nixon resigned in disgrace.

Yet the extent of electronic surveillance under the administration wasn’t revealed until December 1974, when the *New York Times* published a front-page story by Seymour Hersh under the headline “Huge C.I.A. Operation Reported in U.S. Against Anti-War Forces.” The article exposed part of Nixon’s spying under a program code-named “Operation MINARET,” which made use of the cables the NSA searched via SHAMROCK and by capturing radio transmissions.

Congress was shocked. During the investigation led by Sen. Church in 1975, Congress discovered that the NSA had access to communications involving millions of Americans and that there were about 1,200 Americans on watch lists, mostly people opposing the Vietnam War.

But the names of some Americans on the watch list were kept sealed until they were released this September. The newly declassified documents reveal that the NSA’s spying targeted prominent Americans even before Nixon took office. According to the National Security Archive, the NSA “eavesdropped on civil rights leaders Martin Luther King and Whitney Young, as well as boxing champion Muhammad Ali, *New York Times* journalist Tom Wicker, and *Washington Post* columnist [and humorist] Art Buchwald”—and Sen. Church himself.

In response to Sen. Church’s investigation, Congress passed the Foreign Intelligence Surveillance Act (FISA) of 1978, over the objections of a few hard-liners in the Ford administration, including Laurence Silberman. It was intended to ensure that the NSA was focusing on foreigners and not on Americans, and “to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination
that national security justifies it.”

FISA barred the NSA from intentionally acquiring radio signals of the domestic communications of Americans without a warrant. It also barred the NSA from acquiring wire communications here that were to or from Americans, whether intentional or not. And it barred the NSA from intentionally targeting radio communications to or from a known U.S. person in the country. It also created rules for obtaining warrants to target Americans, requiring probable cause that a person was knowingly aiding an agent of a foreign power or someone planning “terrorism” or sabotage, as well as short-term rules for emergency or war.

Congress also created a special court, the Foreign Intelligence Surveillance Court (FISC), to hear these warrant requests. At the same time, Congress established permanent Senate and House Intelligence Committees to conduct oversight of the NSA, CIA and more.

Project MINARET and Operation SHAMROCK were said to be terminated when FISA passed, and the public believed such activities were barred. By almost all accounts, the NSA was directing its powerful surveillance tools outside of the United States, discarding Americans’ communications that were not relevant to its operations, and tuning its radio channels to foreign navies and diplomats. Meanwhile, a Soviet reformer named Mikhail Gorbachev came to power, the Cold War thawed, the Berlin Wall fell, and the need for enormous military and intelligence budgets was being questioned.

Then came 9/11.

**Checks and balances?**

This much is clear: In the weeks following 9/11 a handful of men in the Executive Branch literally rewrote our rights as citizens. While Americans were sold war to secure “freedom” against al Qaeda, our freedoms at home were deliberately undone in the name of protecting us.

That revision of our rights occurred on two fronts. One was a public debate over the Patriot Act, which obscured the second: even more dramatic changes being orchestrated by Vice President Dick Cheney’s office behind the scenes.

As the Pentagon prepared for war in Afghanistan and Congress passed an “Authorization for the Use of Military Force,” the George W. Bush administration sent Congress a wish list of changes to the law that were later titled “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,” otherwise known as the “USA Patriot Act,” or Patriot Act.

The Patriot Act changed some parts of FISA, but nowhere did it authorize the NSA to acquire all of Americans’ phone or internet records. Nor did it change FISA’s rules to allow Operation SHAMROCK-style monitoring of the content of Americans’ international communications.

While Congress was considering the Patriot Act, the White House had already secretly changed the rules for NSA surveillance on these shores. Arch-autocrat David Addington (Vice President Cheney’s right-hand man) hand-picked one Justice Department official—the newly hired John Yoo—to write a legal memo justifying the NSA surveillance programs that Edward Snowden would expose 12 years later. Yoo wrote a secret memo asserting that the president is not bound by FISA’s legal rules for warrants because he has plenary powers as commander in chief.
Attorney General John Ashcroft, who was busy pushing the Patriot Act, did not even know Yoo had written that memo about what became known as the “President’s Surveillance Program” when he cosigned the president’s first authorization document on Oct. 5, 2001 and the NSA began asking telecommunications companies for access to their switches.

It was two years after the launch of the new NSA surveillance before the White House told even one judge on the Foreign Intelligence Surveillance Court (FISC) about the programs. That judge, the chief judge, was not asked to approve the surveillance and was not allowed to tell the other FISC judges about it.

In 2004, the Justice Department hunkered down to create a new legal memo rationalizing the program as implicitly authorized by the Authorization to Use Military Force in Afghanistan. Later that year, the FISC was asked to approve an order authorizing this surveillance for the first time, and it did.

While this battle was brewing and the presidential election was in full swing, James Risen and Eric Lichtblau of the New York Times were onto a story about the NSA’s domestic surveillance, but the White House claimed the story would hurt national security and risk American lives, and so publisher Arthur Ochs Sulzberger, Jr. held it until more than a year after the election.

On Dec. 16, 2005, the Risen-Lichtblau story broke: “Bush Lets U.S. Spy on Callers Without Courts.” The Bush administration responded by declassifying the least controversial component of the program and rebranding it as the “Terrorist Surveillance Program,” or TSP. As Bush famously quipped in trying to distract from the revelations: “If somebody from al Qaeda is calling you, we’d like to know why.”

In the midst of the uproar over the NSA spying, the Patriot Act was reauthorized in March 2006.

But in May of that year, more leaks came, with USA Today publishing a story that said the NSA was “amassing information about the calls of ordinary Americans—most of whom aren’t suspected of any crime.”

By the time these extraordinary surveillance programs had been operational for six years, nearly 3,000 unelected executive branch employees (and an unknown number in the private sector) knew of the programs, but only 60 out of the 535 members of Congress.

Nevertheless, in 2007, aided by lobbying from telecommunications companies like AT&T—which feared it would be held criminally or civilly liable for violating the Wiretap Act and FISA — Director of National Intelligence Mike McConnell began a full-court press to get FISA changed to give retroactive immunity to the companies and Congress’s blessing to the programs. After a court struck down a portion of the program, McConnell demanded Congress temporarily authorize it through the Protect America Act, which was replaced a few months later in 2008 by the FISA Amendments Act.

Then-Sen. Obama, despite expressing earlier concerns about the NSA’s warrantless electronic surveillance, supported those bills as he began to seek the White House. As president, he has embraced those (and other) controversial uses of power that were initiated by the Bush administration. Although he immediately sought to shut down Guantánamo, only to be thwarted by Congress, on the issue of NSA spying he has largely continued the programs and
defended them. There has been little “change” or “hope” when it comes to protecting Americans’ privacy from the NSA’s surveillance powers. It’s been mostly business as usual under for the NSA, FBI and DHS.

Moreover, in light of the full weight of the Snowden revelations, when one looks at the statutory constraints on the NSA now, the limits in FISA that ostensibly protect Americans’ rights look slippery.

For example, Section 702 of the FISA Amendments Act repeats the traditional rule that the NSA cannot acquire communications that “intentionally target any person known at the time of acquisition to be located in the United States.” Given the revelations, though, does this mean the statute allows targeting of Americans in pools of information after international communications are seized?

Similarly, the NSA “may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” However, at the time an email is transmitted and thus acquired, the NSA could argue that it does not know where all the recipients are located, as a Bush rep argued “hypothetically” to privacy advocates in 2007.

Thus the protections in the FISA statute that at first appear to be shields against spying on Americans, appear upon closer inspection to operate as swords.

Where’s the Fourth Amendment?

Three rulings issued by FISA judges hand-picked by the Chief Justice have narrowly construed people’s Fourth Amendment rights when it comes to two core issues: the rules for content and data acquired by the NSA.

The Bush administration set the stage for its evasion of the Fourth Amendment in 2002, when it asked for a ruling from the FISA Court of Review (FISCR), which oversees FISC, in a case involving a Patriot Act provision changing the purpose of FISA surveillance. Judge Silberman (who testified against FISA in 1978) and two other judges heard government arguments—arguments originally concocted by Yoo. Silberman acted like an advocate from the bench, arguing that the Constitution does not require a warrant before the government can acquire the content of Americans’ communications.

The FISCR ruling opined that the constitutional test for searches in intelligence cases was “reasonableness,” not a warrant, and “the key to the reasonableness of any search is the exterior threat.” In 2008, an unnamed “Internet Service Provider” (ISP) challenged “directives” issued after FISA Amendments Act as unconstitutional, but the FISCR ruled that the Constitution did not require a warrant based on probable cause to demand content of communications. In balancing whether a search order was “reasonable” under the Fourth Amendment, the court ruled that national security is of the “highest order of magnitude.”

In the most recent decision issued by the FISC, a lower court judge ruled that the NSA could acquire Americans’ call records en masse because Americans have “no reasonable expectation of privacy” in their phone or Internet data—a claim based on a Supreme Court decision from 1979 that most Americans have never heard of.

In that obscure case, Smith v. Maryland, a robbery suspect named Michael Lee Smith sued the state after police obtained his call records from his phone company without a search
warrant. The Supreme Court, dominated by four new Nixon appointees, ruled that Smith had no constitutional expectation of privacy in information about himself conveyed to a third party, such as the phone company. (Justices Thurgood Marshall, Potter Stewart and William J. Brennan, Jr. dissented, noting that using a telephone does not carry with it an assumption that this information will be released to others, let alone the government.)

The FISC embraced this precedent despite dramatic changes in technology since the original decision. In the old days, the numbers you dialed could be obtained by law enforcement through a court order, without accessing the content of the conversation. But in the digital age, if the government has access to the calls as they transit the phone company in fiber optic cables, the government can duplicate the content as it seizes data.

Despite these differences, the FISC ruled that Americans’ electronic call records can be vacuumed up by the NSA.

Additionally, the court servilely stated that the NSA’s computers work best when they have records of all of your calls—so all the call records they must have.

The FISC also claimed that the surveillance was consistent with the statutory rules for access to third party records, as modified by the Patriot Act, which allow courts to order businesses to turn over records “relevant to an authorized investigation.” The court’s order deemed all Americans’ phone records to be relevant to a general investigation to prevent terrorism because any record might be a link to a potential terrorist.

If everything is relevant or potentially relevant, then relevance means nothing.

**Now what?**

The good news is that Americans are rejecting these rationales and are doing so in a way that transcends traditional political party divides. A growing number of Americans dissent from these policies. Most Americans know they have should have a right to privacy in their communication and Internet records. A growing number of Americans believe that the content of their emails, phone calls and Internet searches should not be given to the NSA if they have done nothing wrong.

No government agency should be allowed to access the backbone of America’s communications infrastructure inside or outside the United States.

Two of the most recent directors of national intelligence, James Clapper (USAF-ret.) and Mike McConnell (USN-ret.) have led efforts to turn the NSA inward on Americans and have misled Americans about the scope of these powers in the name of keeping us safe. Both cashed out their military service with the private-sector consulting firm of Booz Allen Hamilton (Edward Snowden’s former employer) and then moved to top government “civilian.”

Concerns about trusting the NSA are only underscored when the government has been deceptive in its communications with the American people and with congressional and judicial overseers. In March, Sen. Ron Wyden (D-Ore.) asked Clapper: “Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?” Clapper replied stoutly, “No, sir.”

This denial was exposed as a demonstrable lie four months later, when the Snowden materials surfaced.
The NSA should only be allowed to access the contents of Americans’ calls or emails based on an individualized warrant predicated on probable cause of wrongdoing. As for international calls and emails to or from an American, they should be subject to the requirement of an individual warrant on one end before they can be searched.

No American’s name should be queried in the NSA database of calls, emails and Internet searches without an individualized warrant.

Americans’ phone and Internet data should not be acquired at all, unless it is directly connected (in one or two hops) to a specific person who is a legitimate target of a terrorism or espionage investigation.

We also need better protections for information we have already “shared” with a company—including the data that trails you as a result of digital communications—to protect our inherent right to privacy against both the private sector and government.

As Sen. Sam Ervin (D-N.C.)—a staunch advocate of civil liberties despite his Southern segregationist roots—said in 1974 after investigating government spying on Americans, “Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.”

ABOUT THIS AUTHOR

Lisa Graves is the Executive Director of the Center for Media and Democracy and formerly served as Deputy Assistant Attorney General at the U.S. Department of Justice and as the Senior Legislative Strategist for the American Civil Liberties Union on national security issues. She has been called to testify before Congress as an expert witness on national security and civil liberties issues.

In these times. With liberty and justice for all...
Ralph Nader | Opting Out From the Corporate State of Surveillance


Nader writes: "America was founded on the ideals of personal liberty, freedom and democracy. Unfortunately, mass spying, surveillance and the unending collection of personal data threaten to undermine civil liberties and our privacy rights."


Germany, Brazil to Propose Anti-Spying Resolution at UN. Reuters

Oct. 26, 2013, RSN

Excerpt: "Germany and Brazil are drafting a U.N. General Assembly resolution that would demand an end to excessive spying and invasion of privacy after a former U.S. intelligence contractor revealed massive international surveillance programs, U.N. diplomats said on Friday."


GCHQ and European Spy Agencies Worked Together on Mass Surveillance. Julian Borger, Guardian UK 02 November 13 Reader Supported News

Borger reports: "The German, French, Spanish and Swedish intelligence services have all developed methods of mass surveillance of internet and phone traffic over the past five years in close partnership with Britain's GCHQ eavesdropping agency."

READ MORE

November 12, 2013

Tomgram: Engelhardt, A Surveillance State Scorecard
Mistaking Omniscience for Omnipotence

In a World Without Privacy, There Are No Exemptions for Our Spies

By Tom Engelhardt

Given how similar they sound and how easy it is to imagine one leading to the other, confusing omniscience (having total knowledge) with omnipotence (having total power) is easy enough. It’s a reasonable supposition that, before the Snowden revelations hit, America’s spymasters had made just that mistake. If the drip-drip-drip of Snowden’s mother of all leaks -- which began in May and clearly won’t stop for months to come -- has taught us anything, however, it should be this: omniscience is not omnipotence. At least on the global political scene today, they may bear remarkably little relation to each other. In fact, at the moment Washington seems to be operating in a world in which the more you know about the secret lives of others, the less powerful you turn out to be.

Let’s begin by positing this: There’s never been anything quite like it. The slow-tease pulling back of the National Security Agency curtain to reveal the skeletal surveillance structure embedded in our planet (what cheekbones!) has been an epochal event. It’s minimally the political spectacle of 2013, and maybe 2014, too. It’s made a mockery of the 24/7 news cycle and the urge of the media to leave the last big deal for the next big deal as quickly as possible.

It’s visibly changed attitudes around the world toward the U.S. -- strikingly for the worse, even if this hasn’t fully sunk in here yet. Domestically, the inability to put the issue to sleep or tuck it away somewhere or even outlast it has left the Obama administration, Congress, and the intelligence community increasingly at one another’s throats. And somewhere in a system made for leaks, there are young techies inside a surveillance machine so viscerally appalling, so like the worst sci-fi scenarios they read while growing up, that -- no matter the penalties -- one of them, two of them, many of them are likely to become the next Edward Snowden(s).

So where to start, almost half a year into an unfolding crisis of surveillance that shows no signs of ending? If you think of this as a scorecard, then the place to begin is, of course, with the line-up, which means starting with omniscience. After all, that’s the NSA’s genuine success story -- and what kid doesn’t enjoy hearing about the (not so) little engine that could?
TIME TO END THE SPYING GAME


Americans are justifiably upset about the NSA’s sweeping domestic surveillance. But we should be just as concerned about spying on foreigners.


#9 DELETE SOME OF THE FRONT STUFF AND ADD PRESIDENT O’S ADDRESSES

Contents of #3  Oct. 25, 2011
Arkansas Police Cell Phone Surveillance
Patriot Act, Cyber Surveillance
Books
   Fuchs on Internet
   Landau on Wiretapping
   McCoy on Empire
Fuchs, et al., Internet and Surveillance
Mass Surveillance and False Positives
Databases on Everybody Legislation
IPhone Records
New Photo Tech
Lt. Dan Choi

Contents of #4  Jan. 31, 2012
Obama’s State of the Union Speech
Spying Boon to Corporations vs. Privacy
ACLU: FBI Mapping US
Space Surveillance
NSA Warrantless Surveillance
Muslims Demand End of Surveillance

Here is the link to all OMNI newsletters:  http://www.omnicenter.org/newsletter-archive/

Contents of #5 June 9, 2013
Warrantless Spying: Contact Pryor and Boozman
   Lockshin, Credo Action
   Friday, BORDC
Massive National Security Agency Spying
Massive Surveillance State
NSA Lying, Has Our Emails
Bromwich, Secret Surveillance of All Communications in US
Cybersecurity Act vs. Privacy
Baldwin, Protection from NSA
Take Action to Defund the Massive NSA Spy Center in Utah
Kuzmarov, Modernizing Repression
McCoy, Policing the Empire
Huggins, Political Policing Latin America

Contents #6 July 22, 2013
Ellsberg, Join ACLU Action
Petition to President Obama
Jimmy Carter, US Democracy

SNOWDEN
Greenwald, Edward Snowden
Majority Would Prosecute Snowden, Pew Research Center
William Blum on Snowden, NSA History, CIA, Whistleblower
   Philip Agee (Anti-Empire Report #118)
Greenwald, Lack of FISA Oversight
Sign Petitions on Snowden, NSA, FISA
The Nation, Snowden vs. Surveillance Net and End of Privacy
Lindorff, Not China But US is the Great Hacker
Snyder, “Maincore”: US Martial Law Detainee List
Harris, The Rise of the America’s Surveillance State
Surveillance Cameras
Greenwald, Future Surveillance
Solomon, Effective Resistance

New York Times Reports on Surveillance. For example, Lichtblau (NYT), Data-Gathering Law Widened. ADG (7-6-13) 1A.

END SURVEILLANCE CIVIL LIBERTIES NSA NEWSLETTER #9

--
Dick Bennett

Newsletters
http://www.omnicenter.org/newsletter-archive/

Index:
http://www.omnicenter.org/omni-newsletter-general-index/

National/International Days
MY NEW EMAIL ADDRESS
j.dick.bennett@gmail.com
(479) 442-4600
2582 Jimmie Ave.
Fayetteville, AR 72703