Canada
United States
NORTH PACIFIC OCEAN
NORTH ATLANTIC OCEAN
SOUTH PACIFIC OCEAN
SOUTH ATLANTIC OCEAN
BRAZIL
Chile
rb

EVERY MOVE YOU MAKE

BY JAMES BAMFORD

OVER EIGHT YEARS, U.S. PRESIDENT BARACK OBAMA HAS CREATED THE MOST INTRUSIVE SURVEILLANCE APPARATUS IN THE WORLD. TO WHAT END?

ILLUSTRATIONS BY RAYMOND BIESINGER

THIS SUMMER, AT 1:51 P.M. ON SATURDAY, June 11, an unearthly roar shattered the afternoon quiet along the Florida coast. On Cape Canaveral, liquid fuel surged through the thick aluminum veins of a Delta IV Heavy rocket nearly as tall as the U.S. Capitol. Two million pounds of thrust in three symmetrical boosters fired the engines, sending the craft hurtling over the Atlantic Ocean into the heavens. Eighty seconds after takeoff, it hit Mach 1, the speed of sound.

The Delta IV Heavy, introduced in 2004, is the most powerful rocket in American history, and this was only the ninth time it had launched. Even more exclusive, however, was its top-secret cargo: Inside its nearly seven-story-high nose cone was an Advanced Orion, the world's largest satellite. About eight hours after launch, when the most advanced spy craft ever built went into geosynchronous orbit, it unfurled its gigantic mesh antenna, larger than a football field, and began eavesdropping on the Earth below.

The mission's patch, dubbed "epic/terrifying" by the *Verge*, depicted a masked, armored knight standing defensively before an American flag. A sword strapped to his back bore a cross-guard resembling a set of claws. According to the National Reconnaissance Office (NRO), the intelligence agency responsible for the satellite, the image delivered "a message of tenacious, fierce focus ... representing extreme reach with global coverage."

In a sense, this was a fitting tribute to President Barack Obama as his administration entered its last six months in the White House. Over his two terms, Obama has created the most powerful surveillance state the world has ever seen. Although other leaders may have created more oppressive spying regimes, none has come close to constructing one of equivalent size, breadth, cost, and intrusiveness. From 22,300 miles in space, where seven Advanced Orion crafts now orbit; to a 1-million-square-foot building in the Utah desert that stores data intercepted from personal phones, emails, and social media accounts; to taps along the millions of miles of undersea cables that encircle the Earth like yarn, U.S. surveillance has expanded exponentially since Obama's inauguration on Jan. 20, 2009.

The effort to wire the world—or to achieve "extreme reach," in the NRO's parlance—has cost American taxpayers more than $100 billion. Obama has justified the gargantuan expense by arguing that "there are some trade-offs involved" in keeping the country safe. "I think it's important to recognize that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience," he said in June 2013, shortly after Edward Snowden, a former contractor with the National Security Agency (NSA), revealed widespread government spying on Americans' phone calls.

Since Snowden's leaks, pundits and experts (myself included) have debated the legality and ethics of the U.S. surveillance apparatus. Yet has the president's blueprint for spying succeeded on its own terms? An examination of the unprecedented architecture reveals that the Obama administration may only have drowned itself in data. What's more, in trying to right the ship, America's intelligence culture has grown frenzied. Agencies are ever seeking to get bigger, move faster, and pry deeper to keep pace with the enormous quantity of information being generated the world over and with the new tactics and technologies intended to shield it from spies.

This race is a defining feature of Obama's legacy—and one that threatens to become never-ending, even after he's left the White House.

THE FOUNDATIONS of Obama's shadow state date back to the immediate post-9/11 period. Six weeks after the attacks, the Patriot Act, which greatly expanded the government's surveillance powers, was rushed through Congress and signed by President George W. Bush. A few months later, the Bush administration created the Information Awareness Office, part of the Defense Advanced Research Projects Agency (DARPA). That led to the development of the Total Information Awareness program, designed to vacuum up vast amounts of private electronic data—banking transactions, travel documents, medical files, and more—from citizens. After the media exposed and criticized the program, which didn't use warrants, Congress shut it down in late 2003. Much of the operation, though, was simply transferred to the NSA.

In 2005, the *New York Times* revealed that Bush had authorized the NSA to monitor the international electronic communications "of hundreds, perhaps thousands, of people in the United States." Codenamed Stellar Wind, the program intercepted telephone conversations, emails, and metadata from taps inside AT&T facilities and from satellites. Each day, millions of communications were scanned for addresses and keywords associated with al Qaeda. Any leads were sent to the FBI. (A secret internal analysis conducted by the bureau in 2006 indicated that no information from Stellar Wind had proved useful.)

The same week the *Times* investigation was published, Obama, then a senator, gave a speech defending civil liberties and asking the Senate to hold off on voting to reauthorize the Patriot Act. "If someone wants to know why their own government has decided to go on a fishing expedition through every personal record or private document ... this legislation gives people no rights to appeal the need for such a search in a court of law," the former constitutional law professor declared. "This is just plain wrong."

Obama rode a wave of negative public opinion on mass surveillance. In January 2006, a Zogby Analytics poll showed that, by a margin of 52 to 43 percent, Americans wanted Congress to consider impeaching Bush if he wiretapped citizens without a judge's approval. Obama then carried the opposition narrative into his White House bid. In late 2007, he publicly promised, "No more secrecy. That's a commitment that I make to you as president.... That means no more illegal wiretapping of American citizens." He even vowed to support a filibuster of any bill that gave retroactive immunity to companies providing assistance to government spies. (PRISM, a secretive program to gather data from major internet companies that was later revealed in Snowden's leaks, was launched in 2007.)

Yet as his campaign progressed, Obama's stance hardened. Overseas, scores of people were being killed in Iraq by suicide bombings; at home, opponents were hammering Obama for being weak on terrorism. Amid this shifting political climate, he brought in John Brennan, a former CIA deputy director, as his top intelligence advisor. During the Bush years, Brennan had supported the very policies Obama campaigned against. Within months, his influence on the candidate was evident. In July 2008, Obama reversed his earlier promises, announcing support for a sweeping surveillance law that largely legalized the NSA's warrantless eavesdropping program and granted immunity to telecom companies that aided in spying.

AMERICA'S INTELLIGENCE CULTURE HAS GROWN FRENZIED. AGENCIES ARE EVER SEEKING TO GET BIGGER, MOVE FASTER, AND PRY DEEPER.

Many of Obama's supporters were horrified. "I am disgusted," one wrote on the candidate's website. "Obama will NOT receive my vote in November." But the Democratic nominee justified his switch by pointing to violent threats in places such as Iraq, Afghanistan, and Pakistan. "In a dangerous world," he wrote on a campaign blog, "government must have the authority to collect the intelligence we need to protect the American people." From a pragmatic perspective, Obama was also heading into the last push for the presidency and needed to appeal to the broader electorate, which viewed terrorism as a bigger threat than his liberal base did.

After being elected, Obama staffed up with intelligence officials who supported mass surveillance. Brennan became his chief counterterrorism advisor (and, a few years later, director of the CIA). Maureen Baginski, the NSA's former director of signals intelligence, a job that had placed her in charge of wiretapping, joined the transition team that helped establish policy for the NSA and other spy agencies.

Most notable, though, was Obama's decision to keep the NSA's chief in place. Keith Alexander, a three-star general who'd led the agency since 2005, was a force to be reckoned with. "We jokingly referred to him as Emperor Alexander—with good cause, because whatever Keith wants, Keith gets," a former senior CIA official told me. "We would sit back literally in awe of what he was able to get from Congress, from the White House, and at the expense of everybody else." Alexander's preferred spying method was blunt. According to a document leaked by Snowden, while visiting Menwith Hill station, the NSA's giant listening post in England, in June 2008, Alexander asked, "Why can't we collect all the signals all the time?" He applied this approach in Iraq, pulling intelligence from phone interceptions, planes, drones, satellites, and other sensors into a powerful computer analysis system known as the Real Time Regional Gateway. He also ran the NSA's massive metadata surveillance program, which involved secretly keeping track of every phone in the United States: what numbers were called, from where, and exactly when—billions of communications each year.

One of the few people with the security clearance to witness Alexander in action was Judge Reggie Walton of the Foreign Intelligence Surveillance Court (FISC). He didn't like what he saw, particularly that the NSA did not have "reasonable and articulable suspicion" to justify monitoring some 90 percent of targets in its metadata program. In a January 2009 opinion, Walton wrote that he was "exceptionally concerned" that the agency was operating in "flagrant violation" of the FISC's orders regarding privacy. Two months later, he accused the NSA of making "material misrepresentations" to the court, which in less polite language is known as lying. He pointed the finger at Alexander, writing that the general's explanation for why his agency had been eavesdropping illegally on tens of thousands of Americans—essentially, that he thought privacy restrictions applied only to certain archived data—"strains credulity." Walton concluded that oversight of metadata gathering "has never functioned effectively."

Yet Obama didn't dismiss Alexander. In fact, the following year, the general was awarded a fourth star and tapped to lead the newly minted, top-secret U.S. Cyber Command. And rather than limit the NSA chief's collect-it-all regime, the president authorized its expansion.

FOR THE OBAMA administration, the next frontier in spying was being able to eavesdrop on every single person in a country by obtaining "full-take audio" of all cellphone conversations. For this new program, code-named SOMALGET, it needed a testing ground. The Bahamas—small, contained, peaceful, 50 miles from the Florida coast—fit the bill.

In 2009, not long after Obama had taken office, the NSA gained access to Bahamian communications networks by subterfuge. The U.S. Drug Enforcement Administration got legal permission to plant monitoring equipment in the nation's telecom systems by convincing the islands' government that the operation would help catch drug dealers. Really, though, it opened a backdoor for the NSA so that it could tap, record, and store cellular data. "[O]ur covert mission is the provision of SIGINT [signals intelligence]," a document leaked by Snowden stated. The host country was "not aware."

Within two years, SOMALGET would achieve its goal of 100 percent surveillance in the Bahamas—all without legal warrants. This included spying on the cell phones of some 6 million U.S. citizens who visit or reside in the country each year; notable celebrities with homes there are Bill Gates, John Travolta, and Tiger Woods.

The NSA didn't stop with the Bahamas, however. It eventually deployed SOMALGET in Afghanistan, which brought the total number of conversations recorded and stored by the program to "over 100 million call events per day," according to leaked agency files. It also began collecting metadata from phones in the Philippines, Mexico, and Kenya. NSA planning documents in 2013 anticipated further uses in other countries.

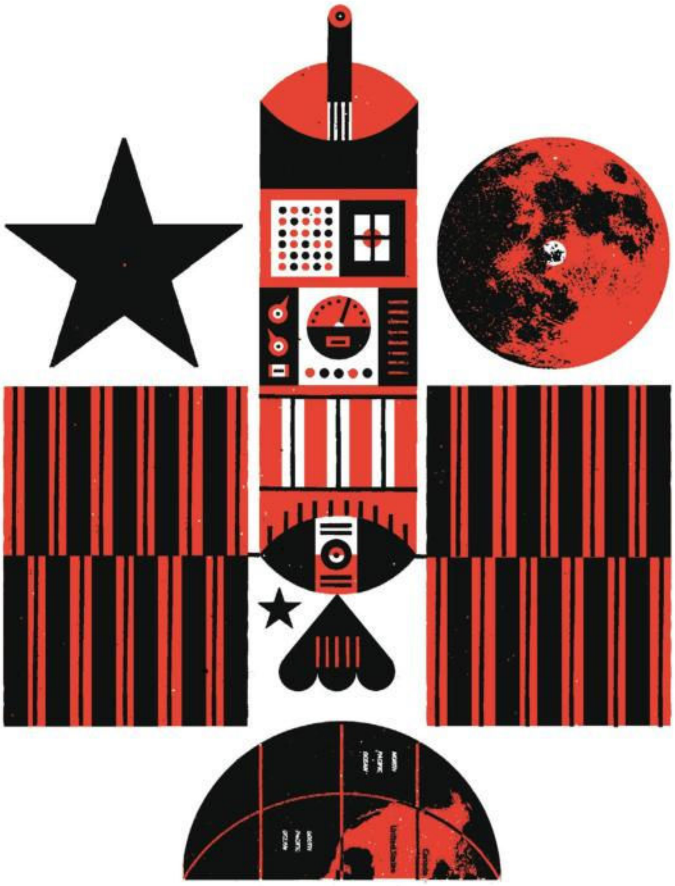
In some cases, the Obama administration cooperated with foreign governments to expand its reconnaissance capabilities. This included members of the Five Eyes, a clandestine alliance of intelligence agencies in the United States, the United Kingdom, Australia, Canada, and New Zealand that dates back to the Cold War. During Obama's first three years in office, the U.S. government paid the British equivalent of the NSA, the Government Communications Headquarters (GCHQ), at least $150 million to enhance surveillance. Because undersea fiber-optic cables from North and South America transit the United Kingdom on their way to Europe and the Middle East, the GCHQ was in an ideal position to place taps on them. It did just that, on cables that could transfer upwards of 21 petabytes of information daily; this included a large slice of the internet, which could be stored for three days before being replaced by new data, and some 600 million "telephone events" every 24 hours. In 2010, not long after becoming operational, the program grew to be so successful that the GCHQ boasted it had the "biggest internet access" of any Five Eyes member. "This is a massive amount of data!" acknowledged an agency PowerPoint later made public by Snowden. Another leaked document declared, "We are in the golden age."

To sift through everything, 250 NSA analysts joined forces with about 300 from the GCHQ. Using computer systems, they searched for data containing any of 71,000 "selectors," such as keywords, email addresses, or phone numbers. Internally, this work was dubbed Mastering of The Internet (MTI). A leaked 2010 GCHQ document stated, "MTI delivered the next big step in the access, processing and storage journey." In a single day, the file continued, a GCHQ surveillance operation known as Tempora had captured, stored, and analyzed some 39 billion pieces of information.

INTO THE NSA'S BLUFFDALE, UTAH FACILITY WOULD FLOW EMAILS, TEXTS, TWEETS, FINANCIAL RECORDS, FACEBOOK POSTS, YOUTUBE VIDEOS, AND TELEPHONE CHATTER.

THE ACCELERATION of surveillance required a construction boom of a scale unprecedented in the history of U.S. intelligence. On March 5, 2012, Alexander opened what is likely the world's largest listening post, about 130 miles north of Savannah, Georgia; members of the press were warned not to bring cameras within two miles. The $286 million, 604,000-square-foot facility has more than 2,500 workstations and 47 conference rooms, and it employs more than 4,000 eavesdroppers and other personnel who focus on the Middle East. Earphones on, facing their computers, employees sit in cubicles and listen to "cuts," or intercepted conversations. "It's very near real time," Adrienne Kinne, a former intercept operator at the complex, told me a few years ago. "We would just get these thousands of cuts dumped on us … [from] Iraq, Afghanistan, and a whole swath of area. We would get [calls in] Tajik, Uzbek, Russian, Chinese."

As of 2013, the NSA had spent upwards of $300 million to expand a former Sony chip-fabrication plant near San Antonio and turn it into the agency's principal listening post for the Caribbean and Central and South America. About 900 miles northwest, it was also constructing a new operations building at Buckley Air Force Base near Denver. The mission was to collect intercepted communications from spy satellites, including Advanced Orions, and ground stations like Menwith Hill, then transmit the data through fiber-optic cables to analysts at their desks near Savannah, San Antonio, and at other NSA outposts. Meanwhile, in January 2012, the NSA opened a $358 million listening post on the island of Oahu targeting Asian and Pacific countries. Upon its debut, Alexander said in a news release that the facility's goal "is to produce foreign signals intelligence for decision-makers as global terrorism now jeopardizes the lives of our citizens, military forces, and international allies."



Not to be left out, Menwith Hill also underwent a multimillion-dollar expansion. Like a moon base hidden in the rolling Yorkshire hills, the station's 33 giant golf-ball-like radomes house parabolic antennas capable of 2 million intercepts an hour from communications satellites. To better analyze data at the post, in 2012, the NSA added powerful supercomputers and boosted personnel from 1,800 to 2,500.

That November, Obama was re-elected following a campaign that centered almost exclusively on domestic and economic issues; little attention was paid to surveillance and privacy. (The Snowden leaks were still more than six months down the road.) Beyond the campaign trail, however, on high ground in Bluffdale, Utah, construction was in progress on the pièce de résistance of Obama's shadow empire. The $2 billion, 1-million-square-foot complex was set to function as the centerpiece of the NSA's global eavesdropping operations. Into it would flow streams of emails, text messages, tweets, Google searches, financial records, Facebook posts, YouTube videos, metadata, and telephone chatter picked up by the constellation of satellites, cable taps, and listening posts by then in operation.

For intelligence analysts, the Bluffdale facility serves as a sort of "cloud," or external hard drive, for intercepted data. About 200 people tend to some 10,000 racks of humming, blinking servers containing trillions of words and thoughts sucked up from unsuspecting people. Some areas of the complex contain data considered critical, such as calls and emails to and from key members of al Qaeda and the Islamic State; other information is eventually erased to make room for more on the servers.

Outside the facility, there's been the occasional protest. In June 2014, a bulbous, 135-foot-long blimp appeared in the sky bearing a giant sign that read, "NSA Illegal Spying Below." Inside were representatives from a coalition of grassroots groups dedicated to privacy. "We're flying an airship over the Utah data center," a written statement from one participating organization, the Electronic Frontier Foundation, proclaimed, "which has come to symbolize the NSA's collect-it-all approach to surveillance."

ALTHOUGH THE EFFORT to gather every possible bit of information follows a certain logic—the more you have, the more likely you are to find what you're looking for—it is complicated by what NSA officials refer to as the three V's. "Inside [the] NSA, we often say that's the volume, velocity, variety issue," Alexander's deputy, Chris Inglis, told an audience of intelligence officials in 2010, "an enormous quantity of information moving ever faster and coming at us in very complex forms."

Obama's surveillance architecture, it seems, has done little to address this multifaceted problem. In fact, it may have made it worse. Privacy hasn't been traded for security, but for the government hoarding more data than it knows how to handle. Kinne, the former intercept operator, described her work as "just like searching blindly through all these cuts to see what the hell was what."

In the wake of the Snowden leaks, administration officials tried hard to justify the secret collection of Americans' telephone records. "We know of at least 50 threats that have been averted because of this information," Obama said during a visit to Berlin in 2013. He offered no specific examples. Alexander, meanwhile, claimed numerous times to the media and in public speeches that "54 different terrorist-related activities" had been thwarted. But he, too, offered no examples.

On Oct. 2, 2013, when called to testify before the Senate Judiciary Committee, the general backtracked. Alexander cited only one instance when an intercept detected a potential threat: a Somali taxi driver living in San Diego who sent $8,500 to al-Shabab, his home country's notorious terrorist group. That winter, a panel set up by Obama to review the NSA's operations concluded that the agency had stopped no terrorist attacks. "We found none," Geoffrey Stone, a University of Chicago law professor and one of five panel members, bluntly told NBC News in December 2013. Since then, despite mass surveillance both at home and abroad, shootings or bombings have occurred in San Bernardino, California; Orlando, Florida; Paris; Brussels; and Istanbul—to name just a few places.

Beyond failures to create security, there is the matter of misuse or abuse of U.S. spying, the effects of which extend well beyond violations of Americans' constitutional liberties. In 2014, I met with Snowden in Moscow for a magazine assignment. Over pizza in a hotel room not far from Red Square, he told me that the NSA puts innocent people in danger. In his experience, for instance, the agency routinely had passed raw, unredacted intercepts of millions of phone calls and emails from Arab- and Palestinian-Americans to its Israeli counterpart, Unit 8200. Once in Israeli hands, Snowden feared, this information might be used to extort information or otherwise harm relatives of the individuals being spied upon.

That September, after my interview with Snowden was published, 43 members of Unit 8200 quit their posts in moral protest. They charged publicly that Israel used intercepted communications, like those sent to it by the NSA, to inflict "political persecution" on Palestinians. They said data were gathered on sexual orientations, infidelities, money problems, family medical conditions, and other private matters and then used as tools of coercion—to force targets into becoming Israeli collaborators, for example. "[T]he intelligence is used to apply pressure to people, to make them cooperate with Israel," one member of the dissenting group, who asked that his name not be used, told the *Guardian*.

The NSA has at least considered employing similar tactics in the United States. In a top-secret memo dated Oct. 3, 2012, Alexander raised the possibility of using vulnerabilities discovered in mass data—"viewing sexually explicit material online," for instance—to damage reputations. The agency could, say, smear individuals it believed were radicalizing others in an effort to diminish their influence.

Obama, meanwhile, has taken virtually no steps to fix what ails his spying apparatus. After the Snowden revelations, the president called for ending the NSA's collection of metadata from phone calls by U.S. citizens. But this represents a rare tremor in the surveillance state. More consistently, Obama has limited oversight. In his first year as president, he threatened to veto a bill from his own party that would have required him to brief all members of congressional intelligence committees about covert operations, as opposed to the much smaller "Gang of Eight," made up of top-ranking party and committee leaders and created in the Bush era to shield illegal activities from scrutiny. Gang briefings, former White House counterterrorism czar Richard Clarke told Rachel Maddow in 2009, were often a "farce."

While keeping critics at bay, the Obama administration has gone after people blowing the whistle on intelligence abuses. The Justice Department has charged eight leakers—more than double the number under all previous presidents combined. "[T]his trend line should be going in the opposite direction," an ACLU lawyer argued in a 2014 blog post. "The modern national security state is more powerful than ever—more powerful even than during the Cold War. It demands democratic accountability."

THE NATIONAL Geospatial-Intelligence Agency (NGA) released a report in June detailing what it calls a "data tsunami." By the end of this decade, there will be anywhere from 50 billion to 200 billion networked devices on a planet of some 8 billion people. "For the intelligence community, this equates to 40 zettabytes of data, or 1 sextillion bytes," the NGA states. "Described in more familiar terms, this is the equivalent of every person on the planet having 174 newspapers delivered daily." Viewed another way, that's more data than 7 billion Libraries of Congress could hold.

In the surveillance state Obama has built, this deluge threatens to bury the few needles that might exist—warnings of attacks, signals of radicalizing groups, rallying cries of extremist recruiters—even deeper in the proverbial haystack. So, too, does encryption: Once a tool used mostly by spy agencies and militaries, encryption is becoming commonplace in everyday digital chatter to keep government eyes and ears out. Gmail offers it. WhatsApp began providing its billion-plus users with automatic encryption in April. In July, Facebook announced that it would soon give the option of end-to-end encryption on its Messenger app. More services will surely follow.

Speed is a critical component in breaking encryption because most codes are based on factoring extremely large prime numbers. Conducting what's known as a "brute force" attack—trying every possible combination of digits—using even the most powerful computers in operation would take centuries or longer to succeed.

Obama, though, signed an executive order in July 2015 urging the creation of an exaflop supercomputer—a machine about 30 times faster than anything in existence. It would be capable of conducting more than a quintillion (1,000,000,000,000,000,000) operations per second. The president's charge to build was mostly targeted at the scientific community; behind the scenes, however, the NSA has been preparing to breach the exaflop barrier since 2011.

That year, the agency secretly built a 260,000-square-foot facility at the Oak Ridge National Laboratory in Tennessee, the same place where the Manhattan Project developed the atomic bomb. Its research focuses on hitting the computing speed that would not only give the agency an edge over encryption, but also provide it with better cataloging capabilities to tackle the ocean of data already arriving daily at complexes like the one in Bluffdale, Utah.

The government is also finding ways to cheat, most notably through Bullrun, a code-named program run jointly by the NSA and the GCHQ. The agencies clandestinely collaborate with technology companies and internet service providers to “insert vulnerabilities into commercial encryption systems,” as reported by the *Guardian*. As of 2010, according to a top-secret GCHQ PowerPoint, the NSA had already achieved a breakthrough: “Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable,” the leaked slides state. By 2015, the British agency hoped to have cracked the encryption of 15 major internet companies.

QUANTUM COMPUTING COULD BE A GAME-CHANGER IN U.S. INTELLIGENCE. IT WOULD BREAK THE LAST LINE OF DEFENSE AGAINST GOVERNMENT INTRUSION.

Looking further into the future, Obama’s NSA has also explored quantum computing—technology that, theoretically, could defeat encryption for good. Its science breaks all the rules. Today, data are stored in binary bits—either ones or zeros—but in quantum computing, so-called qubits could be both one and zero at the same time. This would allow for almost incomprehensible operating speeds. According to documents released by Snowden, the NSA has been working to build “a cryptologically useful quantum computer” as part of a research program broadly called Penetrating Hard Targets.

Ultrafast computing could be a game-changer in U.S. intelligence. It would break the last line of defense against government intrusion. Though this wouldn’t necessarily—or even likely—guarantee that security threats could be identified, it would allow the surveillance state to seize every bit of power that its backers, including Obama, have sought to give it.

After the White House panel set up to review NSA surveillance in 2013 suggested halting efforts to undermine commercial encryption, the president demurred. In a speech—one of the few he’s given on surveillance in his second term—Obama kept to the middle of the political road. “We have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require,” he said. “We need to do so not only because it is right, but because the challenges posed by threats like terrorism, and proliferation, and cyberattacks are not going away anytime soon.”

Zack Whittaker, the security editor for *ZDNet*, summed up Obama’s remarks in a headline: “Keep calm and carry on spying.”

WHOEVER WINS the upcoming presidential election will probably do just that. In response to the Orlando shooting in June, Hillary Clinton said, “I have proposed an intelligence surge to bolster our capabilities across the board with appropriate safeguards here at home”—but offered no details on what that would entail. She has called for Snowden to return from Russia and face trial, and while supporting the end of the NSA’s metadata program, she’s suggested that the agency never broke the law. “I think it’s fair to say the government, the NSA, didn’t, so far as we know, cross legal lines, but they came right up and sat on them,” she told an audience at a San Francisco technology summit in August 2014.

Donald Trump’s rhetoric, meanwhile, suggests that he would prioritize making America’s surveillance empire as powerful as possible. “I think security has to preside, and it has to be preeminent,” he told Fox News in June 2015. Trump has also said NSA reconnaissance is just a fact of modern American life. “I assume that when I pick up my telephone, people are listening to my conversations,” he told radio host Hugh Hewitt last December, implying that Americans should just get used to being spied on.

Whistleblowers, it seems, would not fare well under a Trump administration. “If I were president, [Russian President Vladimir] Putin would give him over,” Trump said of Snowden in a July 2015 appearance on CNN. In 2013, speaking on *Fox & Friends*, he was even tougher. “I think Snowden is a terrible threat. I think he’s a terrible traitor, and you know what we used to do in the good old days when we were a strong country?” Trump asked. “You know what we used to do to traitors, right?” One of the hosts interjected, “Well, you killed them, Donald.” Trump agreed.

This is Obama’s legacy on surveillance: a shadow state of brick and mortar, hardware and software, satellites and eavesdroppers, that is ready to grow on the next president’s command. How big is too big, though, is a question the outgoing president has never answered fully. At what point does gathering data become an end in itself, rather than a means to an end? Is the U.S. government already there or approaching it?

Unless answers come, 50 years from now, the world may look back at Obama’s architecture of surveillance—full of radomes, windowless walls, phone taps, and double-ringed fences—with the same puzzled astonishment that 1950s bomb shelters elicit today. ■

JAMES BAMFORD (*@WashAuthor*) is a columnist for FOREIGN POLICY and the author of *The Shadow Factory: The Ultra-Secret NSA From 9/11 to the Eavesdropping on America*. He also writes and produces documentaries for PBS.