FREEDOM INTERNATIONAL FLORIDA

CONTENTS

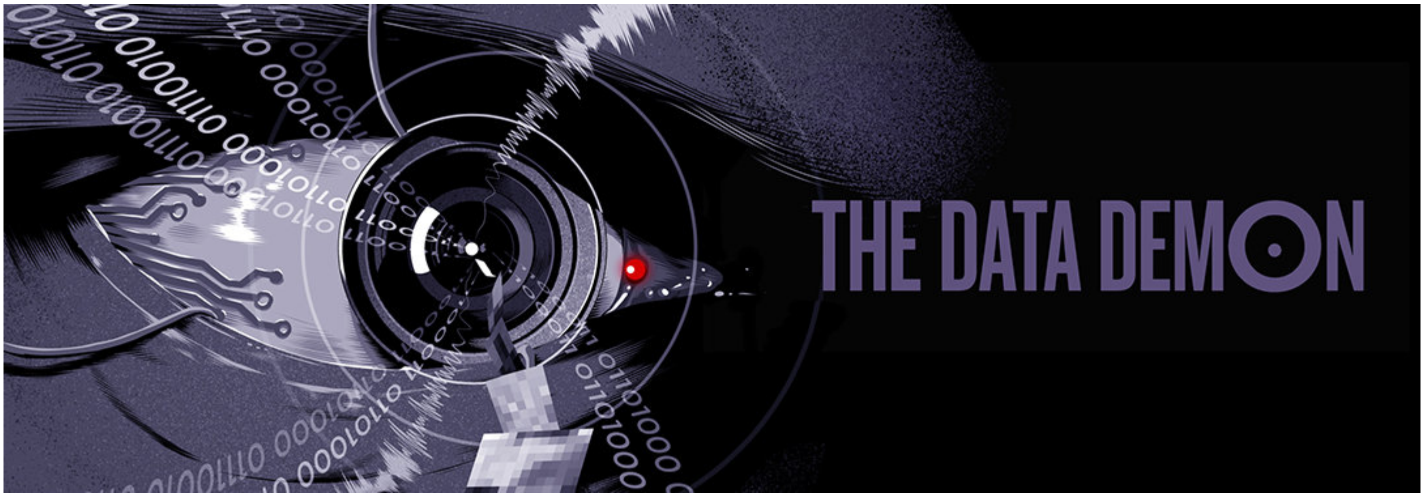


ILLUSTRATION BY CHRIS KOEHLER

PUBLISHED BY
Church of Scientology
since 1968

VOL. 49, ISSUE 1 ▸ COVER STORY

SHARE

The Data Demon

The NSA's monster cybersecurity machine escalates the threat to civil liberties.

BY MARK A. TAYLOR & AJAY SINGH

On a freezing, foggy morning in January 201 1, a tall, thin man with woolly eyebrows and matching hair arrived in Bluffdale, a town of few er than 8,000 people in a bowl-shaped desert valley about 25 miles south of Salt Lake City. Accompanied by several bodyguards, he walked to a white tent pitched on a National Guard training site, where he joined a few high-ranking military officers and politicians in an odd ceremony. Standing in a wooden sandbox with gold-painted shove ls in their hands, the men jabbed at the earth and broke ground on what the local media had dubbed as "the spy center ."

The man was Chris Inglis, then deputy director of the National Security Agency (NSA), the world's largest, costliest and most technologic ally advanced spy or ganization. Its mandate is to keep tabs on activities and individuals outside the United States, as well as terrorism suspects and hostile foreign operations within the nation. The spy center that Inglis inaugurated is a sprawling 20-building complex officially known as the Intelligence C ommunity Comprehensive National Cybersecurity Initiative. Code-named "Bumblehive," the facility opened in 2014 and is popularly referred to as the Utah Data Center.

THE NSA'S EAVESDROPPING
ON THE PRIVATE DIGITAL COMMUNICATIONS OF TENS OF MILLIONS OF AMERICANS STANDS ON SHAKY LEGAL AND CONSTITUTIONAL GROUND.

Richard Brown, dean of the College of Engineering at the University of Utah, calls Bumblehive the "mother of all data centers," not least because it' s a virtually bottomless repository of computer servers at the heart of one of the world' s largest and most ambitious spying projects—tar geted not just at enemy states and potential terrorists but also at friendly nations and millions of Americans.

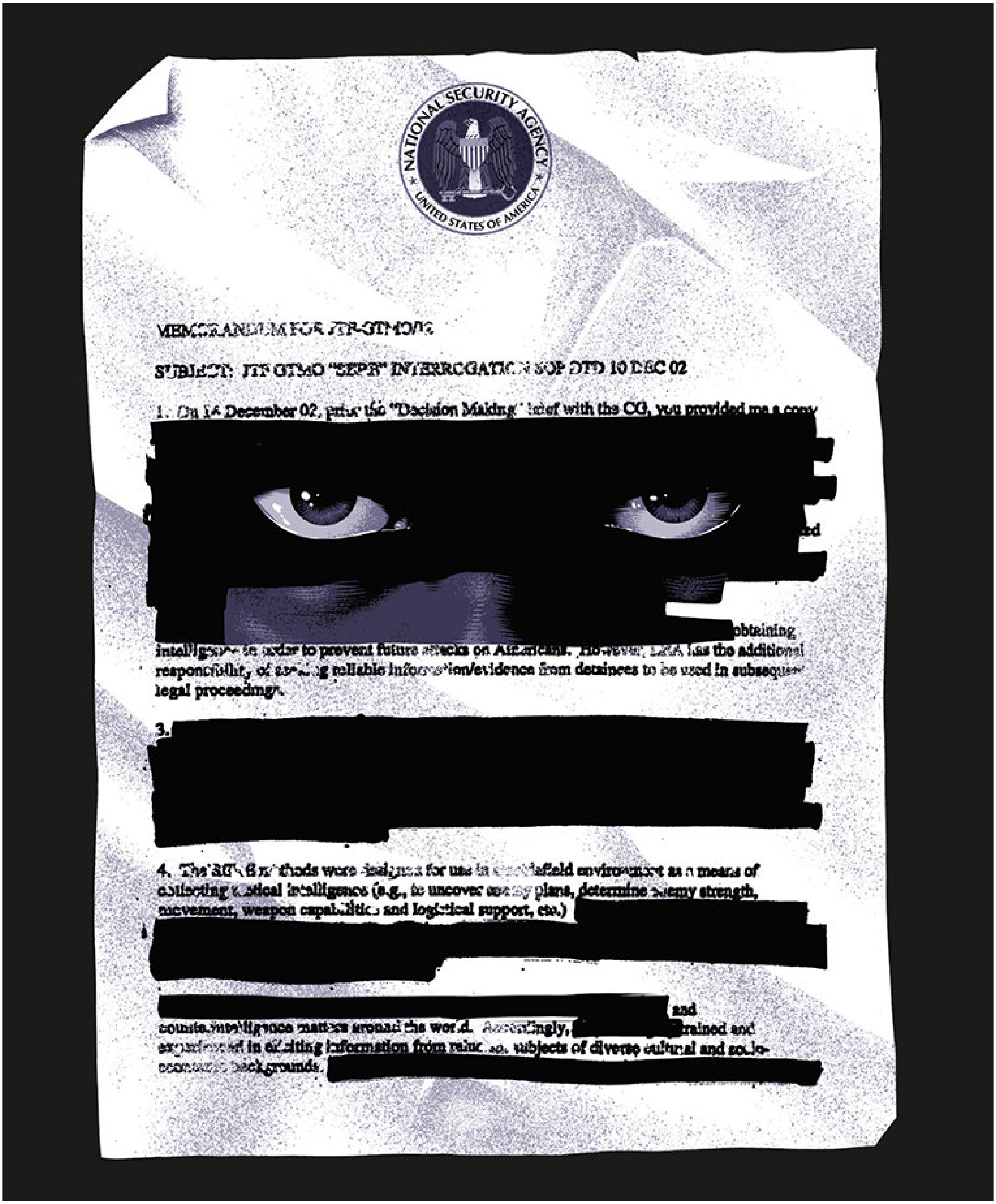
For citizens who have any affinity for civil liberties, there' s one word that describes this vast digital enterprise: scary.

Americans may feel that government snooping is big, but do they know how big? Two-thirds of Americans are concerned about their own government' s spying on citizens, according to respected studies, and 63 percent demand more oversight. The problem is that as an agency whose stock-in-trade is secrecy and surveillance, the NSA and the rest of the government-corporate hybrid intelligence conglomerate specialize in concealing their actions.

That concealment has a handmaiden in major media. The authoritative *Columbia Journalism Review* has reported that the nation' s most powerful newspapers (*The New York Times*, *USA Today*, *Los Angeles Times* and *The Washington Post*) print language that justifies more surveillance, including words that create fear, such as "terrorism," more frequently than they tend to use terms opposing internal spying, such as "privacy" or "liberty."

One of those papers, the *Post,* is owned by Amazon founder Jeff Bezos, who has a $600 million contract with the CIA. Is the *Post* likely to pull punches on coverage of the government spying on citizens? While Amazon issued a statement saying, "We look forward to a successful relationship with the CIA," civil libertarians and media critics were worried—and ur ged the *Post* to mention the deal in every story the newspaper writes about the spy agency .

"If some official enemy of the United States had a comparable situation—say the owner of the dominant newspaper in Caracas was getting $600 million in secretive contracts from the [V enezuelan] government—the *Post* itself would lead the howling chorus impaling that newspaper and that government for making a mockery of a free press," Robert McChesney , one of America's foremost media critics, has commented. "It is time for the *Post* to take a dose of its own medicine."



MEMORANDUM FOR JTF-GTMO/J2

SUBJECT: JTF GTMO "SERE" INTERROGATION SOP DTD 10 DEC 02

1. On 14 December 02, prior the "Decision Making" brief with the CG, you provided me a copy [redacted] obtaining intelligence in order to prevent future attacks on Americans. However, LEA has the additional responsibility of seeking reliable information/evidence from detainees to be used in subsequent legal proceedings.

3. [redacted]

4. The SERE methods were designed for use in a battlefield environment as a means of collecting tactical intelligence (e.g., to uncover enemy plans, determine enemy strength, movement, weapon capabilities and logistical support, etc.) [redacted]

[redacted] and counterintelligence matters around the world. Accordingly, [redacted] trained and experienced in eliciting information from reluctant subjects of diverse cultural and socio-economic backgrounds. [redacted]

ILLUSTRATION BY CHRIS KOEHLER

FOR CITIZENS WHO HAVE ANY AFFINITY FOR CIVIL LIBERTIES, THERE'S ONE WORD THAT DESCRIBES THIS VAST DIGITAL ENTERPRISE: SCARY.

Not likely.

It's no surprise that most Americans have little concept of how much their government knows about them—and what can potentially be done with that information. For example, while most Americans tend to believe the NSA's work is focused on scouring data from overseas to thwart terrorism, the Utah facility's voluminous unfiltered data can be passed on to local police agencies under rules approved by the Obama administration a little more than a year ago.

So should you worry about your phone calls, internet traffic, the programs you watch on TV, your library usage, your online and in-person shopping purchases? The answer is a definite "yes," whether you are guilty of something or not.

And a clue to peeling back the mask of America's Big Brother begins with a look at the NSA's Utah data juggernaut.

"MOTHER OF ALL DATA CENTERS"

Perched on a secluded steppe of the Oquirrh Mountains (pronounced: Oukar) at the southern-most reach of Salt Lake Valley, the Utah Data Center covers more than 1 million square feet. It houses its own water-treatment facilities, 60 huge diesel-fueled emergency standby electric generators and an undisclosed number of computers and servers with unimaginable amounts of storage and analysis capacity. The center uses more than 1.5 million gallons of water daily and consumes enough electricity to power a community of 6,000.

The heavily fortified center's stated purpose is to store vast swaths of the world's communications that have been intercepted from the underground and undersea cables of international, foreign and domestic networks, or turned over by commercial telephone companies or internet social media, data storage or communications servers.

Coursing through thousands of servers and many miles of wiring and routers is the boundless capacity to store all forms of communication. That includes the complete contents of private emails and cell phone calls—replete with their associated metadata—as well as Google searches and so-called "personal data trails" linked to parking receipts, travel itineraries, bookstore purchases and other "pocket litter."

NSA sleuths do not directly process any data at the Utah facility. Instead, the center functions purely for data storage—a digital "cloud" that stores seemingly endless amounts of digital ones and zeros. If that appears to be an utterly unglamorous use for such an expensive facility, it's also a testament to the fact that America's premier spy-gathering apparatus is drowning in metadata: In a single hour, the agency collects and stores data equivalent to 36 times the entire digital collection of the Library of Congress, according to Matthew M. Aid, an NSA expert and visiting fellow at the National Security Archive at

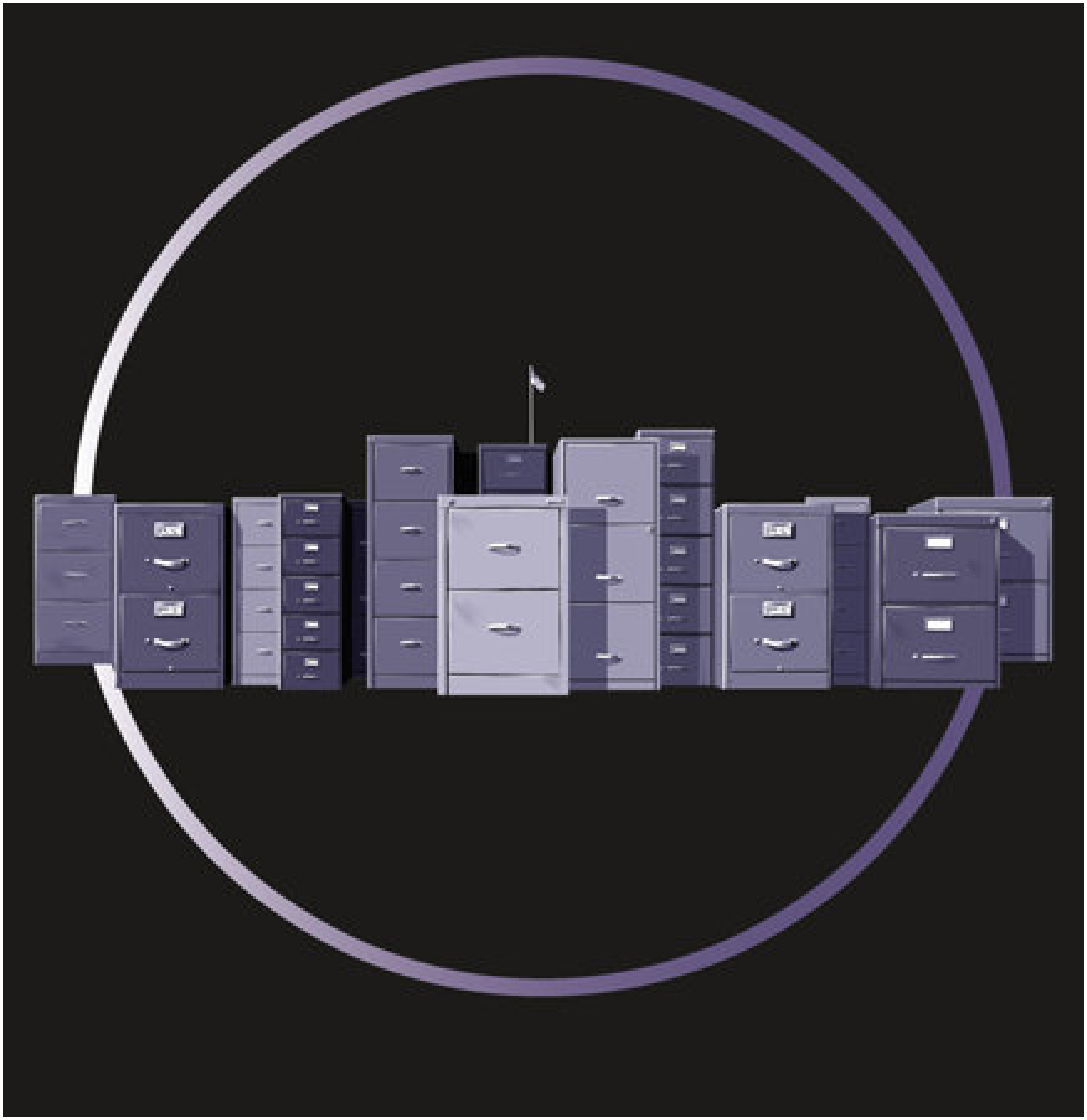


ILLUSTRATION BY CHRIS KOEHLER

IN A SINGLE HOUR, THE AGENCY COLLECTS AND STORES DATA EQUIVALENT TO 36 TIMES THE ENTIRE DIGITAL COLLECTION OF THE LIBRARY OF CONGRESS. [THE LIBRARY OF CONGRESS HAS ARCHIVED AN ESTIMATED 690 TERABYTES—EQUIVALENT TO THE CONTENTS OF ABOUT 690 MILLION BOOKS—OF DATA]

George Washington University, who obtained that statistic from knowledge able sources. (The Library of Congress has archived an estimated 690 terabytes—equivalent to the contents of about 690 million books—of data, adding an average of 5 terabytes per month.)

The Utah center, according to expert NSA watchers, uses a supercharged form of NARUS technology developed by a contractor subsidiary of Boeing Corporation. NARUS can analyze 1.25 million emails of 1,000 words each every second, which equals a staggering 108 billion emails a day.

The data center is able to access financial information, stock transactions, business deals, foreign military and diplomatic secrets, legal documents, confidential personal communications—all heavily encrypted. Many experts believe the NSA has made enormous breakthroughs in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed not only by governments around the world but also by many computer users in the United States.

NSA analysts and computer experts access the data stored in Utah from remote locations that include Washington, D.C., the NSA headquarters at Fort Meade, Maryland, plus a multitude of satellite offices that house NSA contractors.

What makes the Utah Data Center so compelling and controversial, notwithstanding its size and computer capacity, is the work in which it is engaged. Top secret documents leaked in 2013 by whistleblower Edward Snowden—the NSA analyst contractor who worked for a well-known contractor, Booz Allen Hamilton—revealed NSA surveillance programs targeting U.S. citizens without probable cause or warrant from a judge, and in likely violation of the Fourth Amendment to the U.S. Constitution guaranteeing privacy.

One such widely used program, PRISM, extracts contents stored in private user accounts at Yahoo, Microsoft, Facebook, Google and five other internet companies. The once-secret program, which the NSA refers to by other code names, scans through trillions of communications caught in its invisible net, searching minutia such as voice conversations, emails, texts and data sets simultaneously. According to Snowden's revelations in 2013, PRISM was, in the words of U.S. intelligence officials, "the number one source of raw intelligence used for NSA analytic reports." NSA and FBI officials testified that PRISM helped prevent at least 45 terrorist attacks from 2007 to 2013, including plots to blow up the subways under New York City's Grand Central Station and Times Square during rush hour.

> THE BOTTOM LINE ABOUT THE NSA'S BULK SURVEILLANCE ISN'T JUST THAT IT VIOLATES CITIZENS' CIVIL RIGHTS BUT THAT IT CAN ALSO BE MISUSED FOR PURPOSES OTHER THAN COUNTERTERRORISM AND NATIONAL SECURITY.

Another program, Stellar Wind, targets unsuspecting American citizens with warrantless surveillance and data collection activities that involve data mining of communications, including email, telephone conversations, financial transactions and all internet activity. The Dishfire program scans hundreds of millions of texts a day. The XKeyscore program searches and analyzes global internet data and, according to Snowden and investigative journalist Glenn Greenwald, it enables unlimited surveillance of anyone, anywhere in the world.

Some telecommunications giants and internet service providers also assist the agency in hacking. "It's less about designing the software and more about designing systems for inserting the software," explains Aid, the NSA expert. "The software by itself is a relatively simple device—a simple piece of code. The hard part is how to covertly insert it into someone's computer or an email system or communications grid without it being detected."

The NSA is known to have planted digital bugs that have the ability to survive undetected for years in tens of thousands of computers worldwide. The agency does this either remotely or through so-called "interdiction"—the CIA or the FBI intercepts shipments of hardware from manufacturers and retailers, and plants malware in them or installs doctored chips before the computers reach customers. In recent years, the number of NSA bug implants globally grew to 68,975, up from 22,252 in 2008.

But for all that, the NSA's ability to analyze all—or even much—of the data it captures is highly questionable. "Making data useful has been the real challenge for the NSA because it's not exactly easy to process the volumes of information collected through cyberespionage," says Brandon Valeriano, a scholar in international relations at Cardiff University in Britain and the Donald Bren Chair of Armed Politics at the Marine Corps University in Virginia. "It's easier once you know exactly what you're looking for—somebody who has committed a terrorist action. But it becomes very difficult to predict a terrorist action or intervene before something happens."

"EVERYONE IS THE TARGET"

The NSA taps into global communications traffic through secretly attached intercepts placed on the fiber-optic cables ringing the world's ocean floors. Section 702 of the 1978 Foreign Intelligence Surveillance Act (FISA), which is set to expire at the end of 2017, allows the NSA to obtain telephone and internet metadata from such titans of telecommunications and information technology as AT&T, Verizon, Google, Apple, Facebook and Microsoft.

The bottom line about the NSA's bulk surveillance, critics say, isn't just that it violates citizens' civil rights but that it can also be misused for purposes other than counterterrorism and national security. Because the NSA shares data with other agencies such as the FBI—which, in turn, can influence police departments across the nation—law enforcement agencies effectively have access to large amounts of information that is collected as foreign intelligence but could be used to arrest, jail and prosecute citizens for a variety of other reasons.

The Utah Data Center is reportedly a repository for the vast yield of digital surveillance of more than 1.1 billion people worldwide. The upshot, according to University of Utah computer science professor Michael Match, is, "Everyone is the target."

An FBI agent does not need to have any national security related reason to plug your name, email address, phone number or other information into NSA 's colossal database. Agents can examine anyone's private information and if they find something that suggests illegal activity, they can inform local or state law enforcement.

An independent, congressionally mandated, federal privacy watchdog group, the Privacy and Civil Liberties Oversight Board, concluded that the NSA 's programs to collect bulk phone call records and other data has provided only minimal benefit in counterterrorism efforts, is illegal and should be shut down. It said Section 215 of the Patriot Act, which authorizes bulk collection of citizen data, "lacks a viable legal foundation, implicates constitutional concerns under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value."

Not since President Richard Nixon has the NSA turned its spy apparatus on its own population. Created at the height of the Cold War in 1952, the NSA is part of the Department of Defense and the United States Intelligence Community, a federation of 16 separate agencies ranging from the CIA to the Office of Terrorism and Financial Intelligence at the Department of the Treasury.

For many years since its inception, the NSA was secret, jokingly referred to by government and military personnel as No Such Agency. The NSA's existence came to light publicly during the Watergate congressional hearings in the 1970s. The spy agency was also used politically to intercept communications of prominent anti-war and civil rights leaders during the Vietnam War, including senators Frank Church and Howard Baker, and Dr. Martin Luther King Jr., actress Jane Fonda, Dr. Benjamin Spock and many others. The NSA was directed to discontinue such surveillance when an internal review concluded that the practices were "disreputable if not outright illegal."

THE NSA WAS DIRECTED TO DISCONTINUE SUCH SURVEILLANCE WHEN AN INTERNAL REVIEW CONCLUDED THAT THE PRACTICEs WERE
DISREPUTABLE IF NOT OUTRIGHT ILLEGAL.

Today, the NSA's eavesdropping on the private digital communications of tens of millions of Americans stands on shaky legal and constitutional ground. Furthermore, top hackers worldwide—including adversarial governments, rogue nations, corporations, pro- and anti-cyber activists and rich criminal enterprises—are throwing everything they have got at the NSA in attempts to gain access to the data that the agency hoards.

While no bullets are flying, a shadow intelligence-based spy war, fought in cyberspace, is underway. Anyone with a computer and internet access can join in the fray. As former President Barack Obama recently said, “It’s the Wild West. There are no treaties, no international laws, just a patchwork set of emerging norms of what constitutes ac ceptable behavior.”

In Utah, prior to Bumblehive’ s opening three summers ago, state government computer systems were experiencing 30,000 attempted cyberattacks daily . Utah Public Safety Comm issioner Keith Squires tells *Freedom* magazine, “At the time, we thought that many attempts was massive. But after the Utah Data Center opened, that number spiked to more than 300 million attempted attacks against our databases daily. That’s a 10,000-fold increase.” Experts attribute the increase to a beli ef among hackers that they might gain access to the Utah Data Center through any connection it might have to local governmental agencies.

“DIGITAL BLACKWATER” OPERATIVES

No one knows exactly how many private contractors work for the NSA, but the number is estimated to be in the thousands. In 2013, *The Washington Post* estimated more than 1,950 contract companies employing tens of thousands of subcontractors toil for the NSA. Tim Shorrock, author of *Spies for Hire: The Secret World of Intelligence Outsourcing*, says that within national security intelligence circles, NSA contractors are called “di gital blackwater” operatives—a reference to Blackwater Security Consulting, the former name of a highly controversial and occasionally lethal private contractor that reportedly made a fortune from security operations during the Iraq War.

According to the latest Of fice of the Director of National Intelligence report, the projected spending for all U.S. government intelligence is $71 billion, of which an estimated 70 percent is spent on private contractors.

While exact numbers are hard to come by because of government secrecy , Shorrock, who has studied outsourcing of government intelligence for years, estimated a total U.S. intelligence community workforce of 183,000, of which 58,000 are in the private sector .

And, according to a report by the Of fice of Management and Budget, more than a million private contract employees (which would include military and intelligence contractors) hold secret government clearance of some kind—20 percent of all such clearances.

The question is, how did the NSA, the most secretive, important and premiere intelligence spy agency of America’s 16 other agencies, end up being lar gely privatized in the first place?

One part of the answer has to do with technological innovation. In his book, *Spies for Hire*, Shorrock explains that in the 1990s, computer and technological advances developed by high tech entrepreneurs and fledgling companies leapfrogged NSA ’s established telephonic and radar -based surveillance capabilities and threatened to make them obsolete. So, instead of fighting for or competing with the digital revolutionaries, the NSA decided to jump on the bandwagon and benefit from it. Thus began the shadow outsourcing of the agency’ s surveillance and digital intelligence needs to the private sector .

ILLUSTRATION BY CHRIS KOEHLER

THE NSA IS KNOWN TO HAVE PLANTED DIGITAL BUGS THAT HAVE THE ABILITY TO SURVIVE UNDETECTED FOR YEARS.

Another part of the answer—and easily the most important and troubling—is big money , high-level influence peddling, and the well-established revolving door at the center of America's intelligence agencies and government.

In the aftermath of the September 1 1, 2001, terrorist attacks on America, tens of billions of dollars flowed into cyber-intelligence and surveillance. The NSA's budget, which has always been classified, tripled. The agency began recruiting h eavily from the best computer science and engineering programs. It searched private industry in an attempt to poach the most experienced employees. The process destroyed the last vestiges of propriety about public of ficials moving through the revolving door into the lucrative cyber-intelligence security industry .

ILLUSTRATION BY CHRIS KOEHLER

MORE THAN A MILLION PRIVATE CONTRACT EMPLOYEES HOLD SECRET GOVERNMENT CLEARANCE OF SOME KIND—20 PERCENT OF ALL SUCH CLEARANCES.

When high-ranking government officials leave public service to join the ranks of national security contracting, they often take their top-secret security clearances with them. The practice gives them access to the most highly guarded national intelligence secrets in America—and they use the information and knowledge to benefit their corporate employers. Many public officials bemoan the fact that to get the best advice on national intelligence security , the U.S. government has to talk to or consult with private contractors. The shadow intelligence community is now more important than our government agencies.

HEN IN THE FOXHOUSE?

When the U.S. intelligence community recently issued a report on Russian meddling in the November 2016 presidential election, describing not just a concerted effort at electoral interference but a broader attempt to undermine the very idea of American democracy, the NSA quickly elbowed its way to the front of the agencies defending the nation from cyberattacks. For all the money and prestige showered on the NSA, the idea that it should protect U.S. cyberspace is, however, profoundly ironic. This is, after all, the same agency that has been unable to secure its own secrets in recent years.

The most embarrassing breach occurred when Snowden revealed the NSA's secrets three years ago. The NSA subsequently got another black eye when it discovered that two people working at its elite cyber hacking unit, Tailored Access Operations (TAO), allegedly had stolen top-secret hacking tools. One of them, Harold T. Martin III, was arrested in August 2016 and was accused of carrying out the largest theft ever of classified government material in the nation. The other violation of cybertools at the NSA came to light in 2015 but wasn't disclosed until the following year.

THE LAW COULD FACILITATE INVESTIGATIONS INTO GARDEN-VARIETY VIOLENT CRIMES THAT HAVE NOTHING TO DO WITH CYBERTHREATS.

The NSA would be a particularly odd choice for protecting America's corporate sector because the agency would require constant access to the computer networks of companies to safeguard them, which, in turn, would expose a host of data about customers. Such an issue arose in 2014, when Sony Pictures Studios sought the government's assistance following a highly publicized cyberattack on the company's corporate data and employees' personal information, which U.S. authorities blamed on North Korea.

"The idea of a public-private partnership kind of defies all logic and is the kind of thing that happens more in authoritarian countries as opposed to liberal democracies," says Valeriano, of Cardiff University and the Marine Corps University. "The government cannot become a barrier between a cyberattacker and the corporate sector—it's just not the role of the government to protect every person at every time."

Privacy advocates have intensified their criticism of cybersecurity legislation, which encourages government partnership with the private sector. In December 2015, after several failed attempts to come up with legislation that satisfied both national security hawks and privacy critics, then-President Obama signed into law the Cybersecurity Information Sharing Act (CISA). The law enables private companies to share cyberthreat data with seven federal entities, including the NSA and the Department of Homeland Security. Privacy critics have protested that CISA creates a legal framework for companies to monitor internet users more closely and share the resulting data with federal agencies.

Tech industry trade groups also strongly oppose CISA. The Computer and Communications Industry Association stated that while it recognizes the need for government and private sector cooperation in regard to threat assessment, "Such a system should not come at the expense of users' privacy, need not be used for purposes unrelated to cybersecurity, and must not enable activities that might actively destabilize the infrastructure the bill aims to protect."

The law has other problems as well. Although its stated purpose is to prevent terrorism or an "imminent threat of death or bodily harm," CISA could "facilitate investigations into garden-variety violent crimes that have nothing to do with cyberthreats [and are based on] information that was shared under the guise of enhancing cybersecurity," according to Robyn Greene, policy counsel for the Open Technology Institute, a Washington, D.C.-based nongovernment organization devoted to promoting equitable access to digital technology and its benefits.

Indeed, the bulk surveillance of citizens by spy agencies such as the NSA poses serious questions about how governments can misuse personal and other information about individuals. NSA expert Aid says: "The true danger of the NSA is oversight."

Yet, as 2017 opened with a smackdown between incoming President Trump and the intelligence community, it was obvious that oversight is in short supply. Since the NSA is already listening in on Americans, the form of oversight that might make a difference is a citizen chorus telling the spymasters: "Enough!"

« prev
How Much Freedom?

next »
Sean Lawson

FREEDOM

Our Mission

Freedom seeks out and illuminates solutions to society's problems.

Freedom addresses issues, not politics.

Freedom uplifts human aspiration. It stands for accurate and accountable reporting and publishes information available in no other publication.

Freedom is the voice of the Church of Scientology.

Related Sites

LRonHubbard.org
Scientology.org
ScientologyNews.org
WhatIsScientology.org
DrugFreeWorld.org
HumanRights.com
YouthForHumanRights.org
CCHR.org
VolunteerMinisters.org

Freedom Magazine

International Edition
Florida Edition
Media & Ethics
Contact Us
Sitemap

Media Exposés

ALEX GIBNEY & HBO
The Prison of Propaganda

The New Yorker
What a Load of Balderdash

CNN AC360
A History of Lies

INSIDE THE SP TIMES
Merchants of Chaos

BBC PANORAMA
Desperate Lies