Total Information Awareness

By MICHAEL MCCANNE (HTTP://THENEWINQUIRY.COM/AUTHOR/MMCCANNE/)

June 19, 2013

(http://thenewinquiry.com/wp-content/uploads/2013/06/timeisnow.jpg)

Time is Now David Scher (http://davidscher.tumblr.com/post/52411278 is-now-2002-oil-on-canvas) (2002)

The NSA's recent history shows that PRISM is hardly an aberration, but rather the most recent program in the state's continuous search for total knowledge capture

In a rolling valley just south of Bluffdale, Utah, a complex of squat concrete structures is being built. The heavy razor wire fence around the construction site's perimeter is the only hint it's anything out of the ordinary. On Google Earth, there is no construction site at all, only an empty field marked by tire tracks. Someone has labeled the site anyway: "Utah Data Center" floats above this artificially empty space.

In an article for *Wired* (http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/) published in March 2012, James Bradford revealed that the construction site is the future home of the National Security Agency's new digital information mega-warehouse. Bradford — who has long chronicled the secretive agency — claims that, when completed, the center will house the aggregate of all of the NSA's electronic surveillance on thousands of the worlds most advanced servers, holding information measured in hundreds of exabytes (each over a billion gigabytes). The center will use the electricity of a small city to keep those servers going and millions of gallons of water to keep them cool. An array of intrusion detecting sensors will be scattered

around the center's perimeter, backed up by armed guards and K-9 units. Originally called the Community Comprehensive National Cybersecurity Initiative Data Center, the NSA claims it will help protect civilian networks against cyber attacks. However this is neither the NSA's purview (Homeland Security deals with domestic cyber security), nor their interest. Bradford claims the center, when it's completed later this year, will be used to house incredible amounts of intercepted data, taken from both outside and inside the

(http://thenewinquiry.com/wp-content/uploads/2013/06/UDC.jpg) *Google Maps*

's recent revelations, the size and ata Center comes into context. The eaked detail, among other things, an lled PRISM, which sucks up massive amounts of personal information from telecom and Internet companies like Google, Apple, and Verizon and combines them into a single database. Snowden claimed, in an interview with The Guardian, that the PRISM database lets anyone with access monitor and eavesdrop on anyone in the country, drawing on huge troves of captured digital information.

Some congress members, journalists and pundits have expressed shock over the recent revelations about NSA spying, but anyone who has followed the agency's history isn't surprised. The NSA embodies the pure strategic power of information, and the PRISM program — like its various predecessors — is part of a continuous effort to achieve surveillance beyond the limits of laws and existing technology.

The National Security Agency is the largest intelligence service in the world. It evolved from cryptological departments in the military and is responsible for intercepting communications and code breaking — what is called "signals intelligence." Because it is essentially a military organization, its operations are theoretically limited to covering communications from foreign nations or foreign organizations, unless authorized by a warrant from the highly secretive Foreign Intelligence Surveillance Courts (FISC).

During the Cold War, the NSA focused on satellite communications of foreign governments, especially the Soviet Union. After the USSR's dissolution, the focus shifted to terrorist groups, spread across the planet, increasingly connected by digital communication networks. Just as the Industrial Revolution spawned dense proletarian neighborhoods that were fertile ground for conspiracy and insurrection, the Digital Revolution has created a multiplicity of overlapping information networks and encrypted dark webs. In this cyber sprawl, the NSA and other agencies missed chatter leading up to several major terrorist attacks through the 1990s. In the face of these oversights and confronted by burgeoning traffic in digital communications, the NSA sought to upgrade its surveillance capability so that it could peer into every corner of this new virtual territory.

After 9/11, the Bush administration scrambled to set up a program for mass data-collection that would prevent more attacks. They brought in Reagan's National Security Advisor, John Poindexter — infamous as Oliver North's boss in the Iran-Contra affair — to direct the new Total Information Awareness program, and initiated pilot programs to get it up and running. Congress, however, balked at the idea and, citing privacy concerns, scuttled the proposal (and Poindexter's career) in 2003. Undeterred, President Bush secretly directed

the NSA to expand and refine its information gathering in the United States — instructing them to bypass the Foreign Intelligence Surveillance Courts if necessary. With authority from the President and billions of dollars, they set up a secret project called Stellar Wind.

* * *

Digital communications seem to exist as a diffusion of networks spread across the country and interlinked between individuals. This gives them a democratic or even anarchic veneer, but it is deceptive. In reality these networks connect at a limited number of choke points — several pieces of hardware — through which networks are anchored and can be monitored or even shut down, as happened in Egypt and Libya.

Almost all Internet traffic, as well as most phone calls, now moves as coded light over fiber optic bundles called trunk lines. These lines connect at switching centers (peering points) usually housed in telecommunication companies. Most of the world's electronic communications, foreign and domestic, physically pass through a switching center in the United States, making them ideal access points for foreign *and* domestic intelligence.

In 2006, a whistleblower at AT&T disclosed that he had helped set up a secret NSA splitter on one of these peering points in the San Francisco AT&T building. The splitter copies all the digital traffic passing through the line and sends it to a secure room hidden deep within the building. The equipment in that room then copies and processes all the information — Voice over Internet Protocols (VoIP), emails, texts, web traffic, etc. — and transmits it to the NSA for storage. In subsequent lawsuits filled by the Electronic Frontier Foundation, they alleged the NSA had set up these "black rooms" at dozens of telecom and Internet switching stations across the United States.

With these splitters, the NSA's operating principal seemed to have shifted from targeted surveillance to "collect everything and sort through it later." This meant, however, they had to find a way to extract useful intelligence from the vast amount of information gathered. A cottage industry of semi-private firms (like Booz Allen Hamilton, Edward Snowden's former employer) flourished after 9/11, building hardware and systems to compress and analyze information. Meanwhile, the NSA developed algorithms to drive these pieces of hardware, especially programs that could take a suspected individual or target phone number and create a "community of interest," a visualized network of everyone that person or number is connected to.

These programs were developed in part by William Binney, a renowned crypto-analyst for the NSA who spent most of his 30-odd year career breaking and analyzing Soviet communications. After the NSA shifted focus, he was tasked with developing computer algorithms that could sift through the ever-expanding realm of private digital communications. He worked on several of these mapping projects, but when he realized his work was being used — as part of Stellar Wind — to mine domestic communications and spy on Americans, he quit in protest. His story, and the program he helped create, is the subject of a forthcoming documentary by Laura Poitras, who also helped break the recent NSA leaks.

The Snowden affair isn't the first time the NSA's domestic spying has been revealed. In 2006 the *New York Times* — despite threats and appeals from Bush and his administration — exposed aspects of the NSA's extrajudicial wiretapping citing unnamed insider sources including Binney. In the ensuing outcry, Congress investigated the program, and it was brought, ostensibly, back under FISC oversight. But as we now know, the NSA's mass surveillance continued, operating under the legal interpretation that a communication is only "intercepted" when a human reviews the information or listens to the call. Thus the NSA still collects grand swathes of domestic surveillance, organizing it autonomously through various algorithms and storing it away, only needing a FISC warrant when they actually enter a name into their data banks The full extent of this continuing surveillance is impossible to know, but thanks to Edward Snowden much of it is coming to light. Whether PRISM replaced the Stellar Wind program or is just one of its operations remains to be seen.

When President Obama was elected, many hoped he would dismantle the post 9/11 culture of surveillance, conspiracy and unchecked executive power, but it's clear the breadth and scale of state power has only increased since 2008. The Obama administration continues to push for a Haussmannization of cyberspace, demanding that email, VoIP, and social networking platforms construct backdoors and thoroughfares for police surveillance and anti-piracy measures. It has created massive initiatives to carry out cyber war — and may have already participated in the first major cyber attack with the Stuxnet virus. All the while, the NSA and other military intelligence agencies carry on the dream of Total Information Awareness, working at the level of the Internet's very architecture.

* * *

On a technical level, a few hackers, libertarians and software developers are constantly designing programs to hide our virtual identity and protect our digital communications. The Onion Router (Tor) bounces Internet traffic through proxy servers to hide a user's identity, allowing someone to visit proscribed websites without detection or even maneuver around government firewalls, as in China or Syria. The open source Pretty Good Privacy encryption (PGP) is the gold standard for protecting sensitive information — the NSA even recommends it for classified government documents — and, as far as anyone knows, is currently considered unbreakable by even the world's fastest computers. If everyone used PGP, their digital communications would be secure, at least from mass interception. But most people don't use PGP, and encryption software is under attack legally — there have been attempts to ban or restrict its use by private citizens — and physically. The NSA is supposedly building a new supercomputer that will crack current encryption methods using the wide information cache in the Utah Data Center to search for patterns.

Another hope is that the sheer volume of digital information, growing exponentially as millions of people link into the Internet, will simply overwhelm the surveillance capability of even the most technically advanced security services. Perhaps somewhere a rogue programmer is developing applications that will increase this incoherence and overwhelm surveillance algorithms, or perhaps they are creating an encryption standard that is even harder to break.

cal stopgaps, however, and they need to
der questions about the changes in
nance. The NSA is a military
nternet, and its infrastructure, is
rized. This is especially worrisome as,
coming digitally constituted subjects.
nformation and private
o mention our more ephemeral
e fiber optic networks as coded
ngines, Internet service Providers, and
umulate records of where we go,
— which are of course accessible by
the NSA through the PRISM program. CCTV cameras can record our movements in urban spaces, and biometric recognition software can even track our movements autonomously across camera networks.

more or less hidden surveillance, social
and mobile technologies (like Facebook, Twitter, and Google Glass) encourage us to actively self-report our location, affinities, and behavioral patterns, playing on our desire for connectivity and attention. This self-documentation is collapsing the distinction between public and private, and the possibilities for surveillance will only increase as more economic and social functions are digitalized, more CCTV cameras go up, and more objects are embedded with tiny tracking devices (like the radio-frequency identification (RFID) chips that are now embedded in passports and pets) and monitored as part of intelligent logistical networks.

These new technologies allow state power to encode itself into ever-more-minute digital transactions, even if such interactions appear totally benign. State power at its most potent and expansive always appears innocuous. It shapes and controls us not with overwhelming displays of violence but through the administration and surveillance of quotidian social and economic interchanges. As state power fuses with technological innovation, it is harder to actually see it as encroaching, to recognize its broad disciplinary power. It is that very approximation of banality that lends itself to omnipresence.

In the end, we have to examine how we interact with digital information, essentially how we want to live with this technology — or if we want to live with it at all. Most of the debate around the NSA's surveillance programs, when it hasn't been about the moral character of whistle-blowers, usually centers around safeguarding domestic privacy rights while countering terrorism and securing Internet networks, but this misses the larger and more important point. This infrastructure is creating a technological imperium, hidden in the shadows of our digitalized world, regardless of who wields its power or what "democratic safeguards" are put into place.

Intelligence gathering is never benign. It is part and parcel with war making, and domestic spying apparatuses can be seen as preparation to quell any internal threat or rebellion (http://www.guardian.co.uk/environment/earth-insight/2013/jun/14/climate-change-energy-shocks-nsa-prism?CMP=twt_gu), digital or actual. The economic, political and environmental situation in this country — and around the world, from Turkey to Brazil — is rapidly changing, and the promises of industrial capitalism have collapsed. It makes sense that, with no intention to change the

fundamentals of the current system, those in power would prepare the infrastructure to suppress those who might try. In the Utah desert, they are girding themselves for whatever may come, laying the electronic groundwork so that nothing will catch them by surprise. When the Data Center is finished in September, they will be one step closer.

LEARN MORE
ABOUT
TNI *magazine*
(http://thenewinquiry.com/about-tni-magazine/)

NNE
IRY.COM/AUTHOR/MMCCANNE/)

ıtion
s
uiry.com/essays/total-
ırness/)
ng Civil
uiry.com/essays/scenes-
-war/)
ıughter
uiry.com/essays/revolutionary-
)