SURVEILLANCE NATION

The Coming Of The Great American Surveillance State

Published by Solutions From Science

Surveillance Nation
The Coming Of The Great American Surveillance State

A Product of Solutions From Science

The following photos are from Wikimedia commons:
Page 4 - Big Brother poster by Frederic Guimont; ChemicalBit at it.wikipedia [FAL]
Page 31 - Utah Data Center by Tom Sulcer
Pages 36 and 37 - Domestic drones by alftermeyer (Own work)
Page 39 - Domestic drones by U.S. Navy
Page 42 - Information Awareness Office logo by United States Government

TABLE OF CONTENTS

INTRODUCTION

In George Orwell's classic anti-totalitarian dystopian novel "1984," each residence was furnished with a special type of telescreen that functioned as both receiver and transmitter, allowing the government to monitor the activities of its citizens in their own homes on a 24-hour basis.[1] For the Party that controlled Orwell's mythical land of Oceania, this constant surveillance was necessary to ensure that total authoritarian control over the lives of each and every individual could be maintained. Not only would they be able to detect even the slightest hint of revolutionary activity or thinking, but just the presence of so many cameras everywhere was enough to intimidate most into acquiescing to an unjust and repressive ruling order.

If we fast forward to 21st century America, we can fortunately see great dissimilarities between the dark vision of our collective future envisioned by George Orwell and the political, cultural, and social realities that shape people's daily lives in the most powerful nation on earth. The basic forms of democracy have proven resistant to the dubious appeal of revolution and totalitarianism in its various guises, and the freedom to criticize the government and express thoughts and feelings that run contrary to the assumptions and assertions of influential actors and institutions has been fully preserved. In fact, thanks to the rise of modern electronic communications and information-sharing technologies, people's ability to participate in open public debate has expanded far beyond the wildest dreams of even the most enthusiastic proponents of republican democracy from centuries past. Now, it is no longer necessary to head to the nearest public square, street corner, or local meeting of elected legislators in order to make yourself heard. In the digital age, all that is required is an Internet connection and a functioning keyboard, and those who wish to express their most deeply-held opinions on the issues of the day are free to do so in a free-flowing and easily accessible marketplace of ideas that spans the entire globe.

But what many Americans fail to realize is that the United States government has plans for them that are in some ways eerily similar

to the nightmare vision of the future as it was imagined by Orwell more than six decades ago. In the immediate aftermath of the tragic and devastating terrorist attacks of September 11, 2001, Congress and the Bush administration expressed their determination to make sure that such an event would never happen again, and it was out of this concern for the internal security of the country that the project to beef up the country's domestic surveillance infrastructure was born. If anything, the urgency to improve surveillance methods and technologies has actually accelerated under the Obama administration and the new Congress, and while we live in politically contentious times, the dedication of both political parties to protecting America from further terrorist desecration has remained steady and unflinching. So in the name of fighting terrorism and other forms of insidious crime, our elected leaders have given our federal, state, and local police and intelligence agencies permission to set up a system of domestic monitoring, spying, and snooping that far surpasses the efforts of the leaders of Orwell's fictional Oceania in its technological sophistication, analytical abilities, and overall physical scope. While Big Brother spied on citizens primarily through two-way television sets, the modern surveillance system will be relying on the most up-to-date electronic methodologies available to intercept and monitor emails, text messages, chat logs, cell phone calls, search engine queries, and website visits, while also seeking ways to surreptitiously gain access to personal data being stored electronically, either on people's own computers or in the computer systems of private companies with which they have done business.

Needless to say, the U.S. government circa 2012 will be able to gain access to far more sensitive and private information about the lives of its citizens through this comprehensive program of digital surveillance than the Party in Oceania was ever able to pick up by simply looking at people through hidden cameras, since almost everything we do these days interfaces in some manner with the modern electronic communications network that connects us all. In modern America, the hunt for terrorists, heinous criminals, and other dangerous subversives whose nefarious motives threaten to undermine the safety and security of the public, is being used as the rationale for the creation of the perfect surveillance state where everything each and every citizen or non-citizen residing within U.S. borders says or does could ultimately fall under the intense and skeptical scrutiny of those charged with preserving law and order at all costs.

While no one disputes the importance of protecting the country from terrorism, there is plenty of controversy over how we are trying to go about it. Broad bipartisan consensus inside the federal government may

impress observers who seldom venture outside the Washington Beltway, but there are many voices being raised across the country and across the ideological spectrum in opposition to the arrival of the surveillance state, from people concerned that we may be compromising the principles we hold most dear in a futile search for absolute, impregnable security. What unites these critics of pervasive and unrestrained domestic surveillance is their concern over the possibility that giving the police and the intelligence community so much power will inevitably lead to abuses, and these critics sharply object to the idea that sacrificing our basic civil liberties is really necessary in order to keep us safe from terrorism or any other type of crime.

Of course, the governmental authorities responsible for passing the legislation that has facilitated the development of the surveillance state pooh-pooh such fears, insisting that an expansion of internal security measures is perfectly compatible with the United States Constitution. Additionally, the agencies responsible for implementing these policies and developing surveillance strategies insist that safeguards are in place to guarantee that the rights of ordinary citizens will always be protected, even as technologies improve and more and more information about the words, deeds, actions, movements, and locations of every American becomes available for covert perusal.

But as has often been said, those who fail to learn from history are doomed to repeat it. Over and over again, we have seen what can happen when authorities decide that security concerns should override all else. The internment of Japanese-Americans during World War II and the blacklists of the 1950s were motivated by obsessions with internal security, and from the annals of world history we should never forget the outcome of the French Revolution, when an organization called the Committee of Public Safety sanctioned the bloody murder of over 40,000 "enemies of the state" in the name of liberty, equality, and fraternity.[2]

Just to be clear, no one is suggesting that the creation of the new American surveillance state will inevitably lead to the guillotining of thousands in the public square, or that the mere existence of an expansive surveillance capability means that the United States has now abandoned democracy for totalitarianism. What such examples from history are meant to illustrate is that when too much power is concentrated in too few hands, or when we let paranoia and fear guide our actions, there is a real possibility that authorities who started out with the best of intentions may end up trampling all over the rule of law and the rights of law-abiding citizens before everything is said and done.

1942, Arcadia, California. Evacuees of Japanese ancestry line up for lunch at the Santa Anita Assembly center.

When evaluating the dangers that may be looming just over the horizon, it must be emphasized that once the system of spying and monitoring being planned achieves full implementation, police and intelligence agencies will theoretically have unlimited access to mountains of personal data about literally every single individual residing on U.S. soil. And furthermore, all of the sorting, organizing, and analyzing of this information will take place in secret, where it will be left up to the various government agencies involved to decide what, if anything, they are going to do with the data they obtain.

Supposedly, the most that will ever happen is that a new investigation will be opened up by the appropriate authorities if indicators of terrorist or criminal activity should happen to be discovered. But once the government has collected gazillions of gigabytes of information about the habits, ideological beliefs, personal associations, daily movements, financial practices, medical issues, travel histories, charitable donations, online purchases, movie and music preferences, and library reading lists of everyone, the temptation to make use of that data in ways that diverge

from the goals of the war on terrorism could be quite strong indeed. Facile assurances of safeguards being in place aside, U.S. government agencies like the FBI have a long history of carrying out campaigns of harassment and intimidation against activists from the anti-war, anti-abortion, and environmental movements, among other groups. And, thanks to their over-reliance on the flawed "science" of criminal profiling, law enforcement agencies frequently target innocent victims for investigation simply because they fit some preconceived notion of what a villain should look like (i.e. Richard Jewell, the good Samaritan falsely accused of being responsible for the bombing at the Atlanta Olympics in 1996).[3] So the actors responsible for handling all of the highly sensitive information picked up by the surveillance network will be expected to use it wisely and cautiously, even though history suggests that these hopes may be in vain.

Again, it should be emphasized that, at the present time, we are a long way from anything resembling Orwell's infamous totalitarian dystopia. It must be noted, however, that much of the legislation that has been passed in support of the expansion of the surveillance network appears to be designed to do an end run around the Bill of Rights, most specifically the Fourth Amendment. For those whose memories from civics class may have faded a bit with time, this critically important clause asserts that:

> *"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."*[4]

Throughout the history of the republic, this amendment has been seen as the primary constitutional guarantor of the right of privacy. But by relying on a convenient but dubious interpretation of the Fourth Amendment that claims its edicts do not protect citizens from electronic surveillance and monitoring, the government has been pushing the envelope more and more, passing legislation that sanctions widespread collection of personal data from individual Americans while giving institutions and bodies involved in the secret information collection process carte blanche to pursue their mandates any way they see fit. Warrantless searches are even being allowed in some instances, which seems anathema to the entire spirit of the Fourth Amendment. Simply because electronic privacy is not guaranteed specifically in the language of this clause does not mean the concept does not exist, but this is exactly the line of argument that legislators, intelligence agencies, and law enforcement

officials are using to justify massive electronic eavesdropping and data mining schemes to which nothing is theoretically off-limits.

Presumably, if public outrage over the peeling back of privacy rights under the guise of safety were to reach critical mass, Congress and the White House would be forced to respond. This could mean tighter controls over the process by which the private and personal information of the American people is being harvested in the search for that needle in the haystack that indicates some kind of terrorist attack is imminent. The agencies responsible for carrying out surveillance might then be forced to conduct their operations with more circumspection and transparency, thereby reducing the chances of abuse dramatically. But in order for public sentiment to become a factor, it would require aggressive efforts on the part of the mainstream media to inform everyone about what has been happening and what it all might mean. Since September 11, 2001, the establishment media has essentially operated as the propaganda arm for the government's anti-terror campaign and, as the surveillance state has slowly taken shape, it is almost as if the major networks and most influential print publications have been doing everything they can ***not*** to draw anyone's attention to what has been taking place.

Fortunately, independent media has flourished inside the online realm, so it is still possible for individual Americans to discover the truth on their own by visiting websites that are discussing these serious and important issues. But the sad fact is that without the participation of the mainstream mass media, the chances of raising awareness to a level that would actually make a difference are somewhere between slim and none, and slim has already boarded a train heading south. And of course, the more time people spend on websites that are critical of the government, the more likely they will be to run afoul of rogue agencies who will eventually possess the technological means (if they don't have it already) to know exactly which websites everyone is visiting. So even though we still may be a long way from the world envisioned by Orwell, it could be argued that we have at least started down a dangerous road that could ultimately lead to this final destination.

In the wake of the September 11th terrorist attacks, it was inevitable that comprehensive attempts were going to be made to plug the leaks in the country's porous internal security system. But as we assess the rise of this new surveillance regime and examine its specific details and characteristics, there is one question that should remain at the forefront of our minds at all times:

As our government watches us, who will be watching the watchers?

CHAPTER 1:
INVENTING THE CULTURE OF SUSPICION

The September 11, 2001, terrorist attacks scarred the soul of America. Now, some scars heal and other do not; in this particular case, it seems that those in power have been doing everything they can to make sure these wounds are never allowed to completely heal. Whether this desire is driven by uncontrolled paranoia, a real concern for our collective safety, or by some deeper agenda is not entirely clear. Regardless of the motivation, there has been an ongoing attempt over the past 11 years to keep fear and concern over terrorism at the front of our collective thoughts.

This campaign to highlight the potential threat of terrorism has been most apparent in our foreign policy, where the argument has been made repeatedly that it is better to fight terrorists in faraway lands now than to fight them on American soil in the future. But the government's determination to convince us of the ubiquitous and amorphous nature of the terrorist threat is now being used for a different purpose. Now, as a part of the efforts to build the perfect surveillance society, average citizens are being recruited as field agents, assigned to monitor the activities of friends, neighbors, co-workers, casual acquaintances, and strangers on a daily basis, looking for any signs of suspicious behavior. But people are not being asked to watch out for just any old kind of suspicious behavior; rather, they are being encouraged to be on the lookout for any kind of suspicious activity that might indicate that a terrorist plot is afoot.

The Nationwide Suspicious Activity Reporting Initiative (NSI)

No matter how sophisticated technology becomes, in police work, nothing beats good eyewitness testimony. So even though the primary focus in the creation of the surveillance state has been on electronic information interception and diversion, those responsible for this program have also shown a great deal of interest in making much more extensive use of good old-fashioned human intel. But in a time of tight budgets, hiring new personnel is an option that appeals to no one, and given the fact

that terrorists supposedly could be hiding just about anywhere, even if new agents were brought on board, where exactly would they be deployed?

Clearly, the best potential sources of good human intelligence are the American people themselves, who are out and about everywhere from coast to coast and border to border, observing all the things that no one in law enforcement could ever possibly hope to see. But in order to make good use of the information that citizen witnesses might provide, an effective means must be set up for collecting and distributing this vitally important data among all of the various agencies tasked with protecting the nation from terrorist atrocities.

Both the Intelligence Reform and Intelligence Prevention Act of 2004 and President Bush's 2007 National Strategy for Information Sharing called for the creation of a computerized system that would allow state, local, tribal, and territorial law enforcement agencies to share reports of suspicious activity in an open and coordinated manner. As a result, in 2009 the Nationwide Suspicious Activity Initiative, or NSI, was officially launched.[5] Operated from within a special section of the U.S. Department of Justice, the NSI is jointly sponsored by a number of federal law enforcement agencies, including the Department of Homeland Security, the FBI, the Criminal Intelligence Coordinating Council, the Office of Justice Programs, and the Bureau of Justice Assistance, in addition to the DOJ.[6] In the NSI's own words, this program "establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SARs [an acronym for 'suspicious activity reports']."[7]

Under the NSI system, once a police officer or security agent has received a report about some kind of suspicious behavior or activity from a member of the public, after an investigation has been completed, a report will be sent to a nearby fusion center for full evaluation.[8] For those who have not heard of fusion centers, these institutions act as hubs for the collection, analysis, and dissemination of information related to criminal activity with possible national security ramifications.[9] While ostensibly under the authority of state and local law enforcement agencies, fusion centers are also staffed by representatives of federal police organizations who offer training and technical assistance to make sure the data collection process runs smoothly and efficiently. Fusion centers generally maintain a low public profile, but every state has at least one, and it is believed that 72 of these centers in total have been opened across the USA.[10]

If fusion center personnel conclude that a particular SAR is worthy of attention, it will be uploaded into a shared computer network, after

which all local, state, and federal agencies who subscribe to the NSI database will be able to obtain secure access to that data. Theoretically, this will allow any agency investigating possible terrorist-related activity to cross-reference extensively, to see if there is anything happening in the same or other jurisdictions that might suggest an emerging pattern. Highly-advanced computer software can help police personnel sort through extensive collections of information quickly and efficiently, allowing the wheat to be separated from the chaff in a time-sensitive manner.

At first description, this all sounds well and good. But with a system that is relying on human intel to develop its leads and shape its investigations, the methods used to actually collect SARs is of utmost importance. If the leads collected are false or based on a faulty understanding of what is being seen, a system like the NSI database can be hopelessly contaminated with useless or misleading information.

When we look more closely at the methodology being used to convince members of the public to be on alert to what is happening around them, it quickly becomes obvious that a culture of constant suspicion is being brought into being that will likely produce a significant number of spurious suspicious activity reports. Of course, we cannot rule out the possibility that a hidden agenda is at work here, and that creating a climate ruled by paranoia and fear is the real purpose behind the attempts to recruit members of the public as spies in the everlasting and eternal War on Terror.

If You See Something, Say Something

The signature campaign and the most obvious public face of the SAR project is the Department of Homeland Security's "If You See Something, Say Something" initiative. Introduced by DHS Secretary Janet Napolitano in 2010, the stated goal of the program is "to help America's businesses, communities, and citizens remain vigilant and play an active role in keeping the country safe."[11] "If You See Something, Say Something" consists primarily of posters, videos, and audio recordings that warn everyone to be on the lookout for any type of suspicious activity and to report anything they see immediately to the nearest policeman or security guard.

In order to spread the good word—or the bad word, depending on your perspective—the DHS has been forming a series of partnerships with businesses and other private and public organizations, and its announcements and presentations are now playing or are on display in sports arenas, Walmart stores, the Mall of America, Amtrak depots, Metro Transit Authority facilities in New York, Washington, D.C., and Los

Angeles, and in thousands of federal and state government buildings all across the United States.[12] Smaller versions of its posters are available from the DHS website, available for free downloading and printing, so anyone who wants to help support the "If You See Something, Say Something" campaign can do so by hanging these mini-posters in their workplaces, apartment buildings, neighborhood parks, and perhaps even on their refrigerator doors or bedroom walls if they are really enthusiastic about it.

At this stage the DHS is concentrating on recruiting as many corporate partners as they possibly can for this project, and the hope is that "If You See Something, Say Something" posters and announcements will eventually become so commonplace and familiar that they will fade into the background and start to function as a kind of constant subliminal reminder of the great danger we could all face unless people stay on the alert and on guard at all times.

Communities Against Terrorism

It is interesting to note that most "If You See Something, Say Something" materials offer only vague and general references to "suspicious activity" without attempting to define just exactly what this phrase might mean. While there may be a number of reasons for this, one overriding factor could be the desire to avoid any controversy in a campaign that is meant to generate positive publicity for the war on terror, to essentially put a happy face on a project that at its root is based on paranoia and fear. If you start giving specific examples of possible suspicious behavior that might indicate something untoward is about to happen, it might offend those who have benign reasons for doing such things, which could give a bad name to the whole SAR collection process.

But if the "If You See Something, Say Something" campaign assumes a shiny, non-specific patina for the sake of good public relations, the FBI's "Communities Against Terrorism" program takes a much more specific

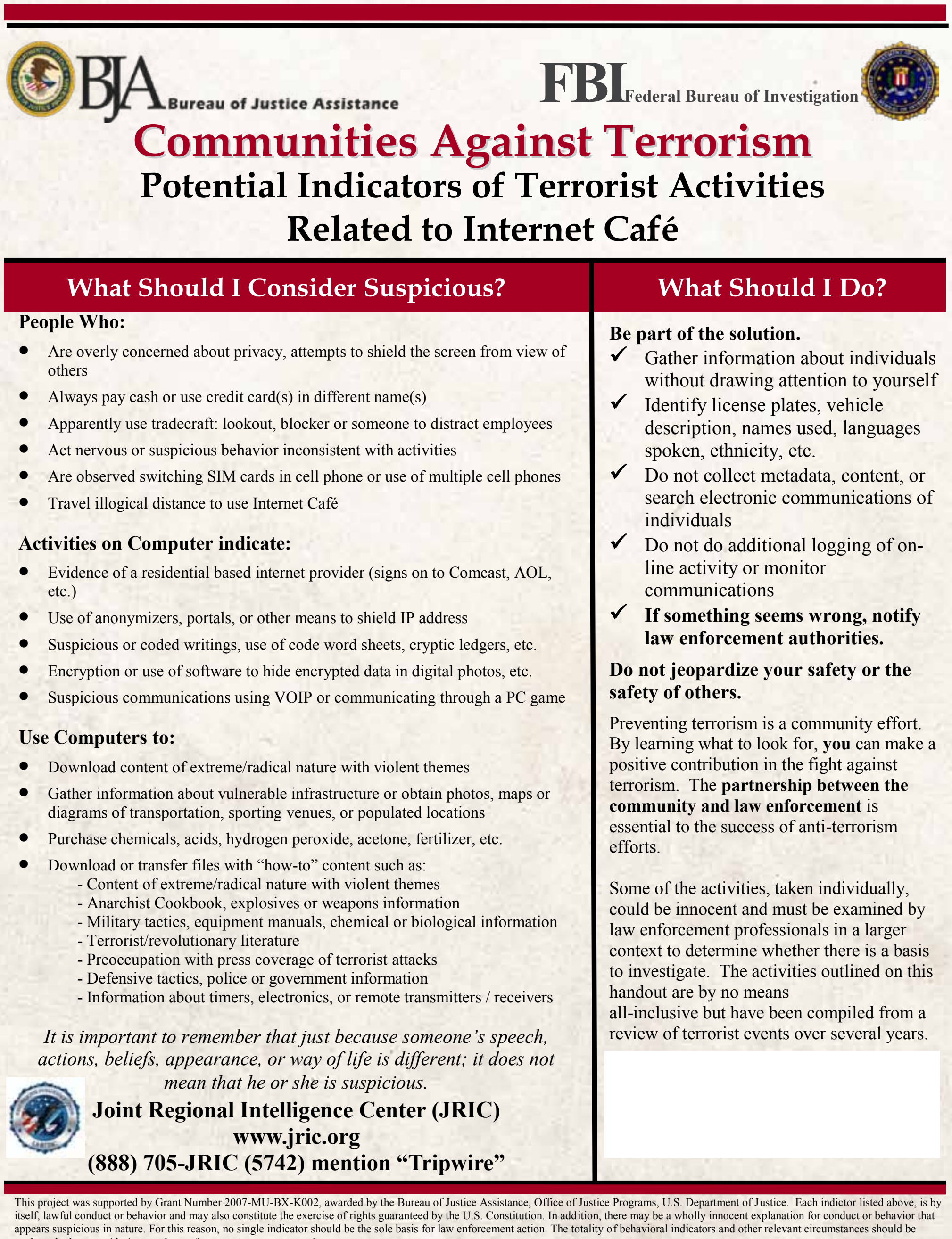
approach, perhaps because its recommendations are for a limited audience and are not meant to be widely shared with members of the general public. Working in conjunction with the Bureau of Justice Assistance, the FBI created a series of leaflets for distribution to owners and managers in 25 different categories of business, warning that terrorists could be active just about anywhere and giving very detailed examples of what "suspicious activity" might actually look like.[13]

The list of businesses that are considered likely to be patronized by potential terrorists includes:

- Airport Service Providers
- Beauty/Drug Suppliers
- Bulk Fuel Distributors
- Construction Sites
- Dive/Boat Shops
- Electronics Stores
- Farm Supply Stores
- Financial Institutions
- General Aviation
- General Public
- Hobby Shops
- Home Improvement
- Hotels/Motels
- Internet Cafes
- Shopping Malls
- Martial Arts/Paintball
- Mass Transportation
- Military Surplus
- Peroxide Explosives
- Recognizing Sleepers
- Rental Cars
- Rental Properties
- Rental Trucks
- Storage Facilities
- Tattoo Shops[14]

As for the content of the FBI's warnings, beneath the Communities Against Terrorism banner, each mini-poster is divided into two sections entitled "What Should I Consider Suspicious?" and "What Should I Do?" Each type of business operation receives a customized description of suspicious behavior and circumstances appropriate for the goods and services they offer. Those receiving fliers are urged to "be part of the solution" and that "if something seems wrong, notify law enforcement authorities."[15]

Curiously, the types of suspicious activities that workers and managers are told to watch out for are a mixture of the specific and the vague, the patently obvious and the almost assuredly harmless. For example, those employed by hotels and motels are advised to be suspicious of customers who request specific room assignments, refuse cleaning service for a



BJA Bureau of Justice Assistance

FBI Federal Bureau of Investigation

Communities Against Terrorism

Potential Indicators of Terrorist Activities Related to Internet Café

What Should I Consider Suspicious?

People Who:

- Are overly concerned about privacy, attempts to shield the screen from view of others
- Always pay cash or use credit card(s) in different name(s)
- Apparently use tradecraft: lookout, blocker or someone to distract employees
- Act nervous or suspicious behavior inconsistent with activities
- Are observed switching SIM cards in cell phone or use of multiple cell phones
- Travel illogical distance to use Internet Café

Activities on Computer indicate:

- Evidence of a residential based internet provider (signs on to Comcast, AOL, etc.)
- Use of anonymizers, portals, or other means to shield IP address
- Suspicious or coded writings, use of code word sheets, cryptic ledgers, etc.
- Encryption or use of software to hide encrypted data in digital photos, etc.
- Suspicious communications using VOIP or communicating through a PC game

Use Computers to:

- Download content of extreme/radical nature with violent themes
- Gather information about vulnerable infrastructure or obtain photos, maps or diagrams of transportation, sporting venues, or populated locations
- Purchase chemicals, acids, hydrogen peroxide, acetone, fertilizer, etc.
- Download or transfer files with "how-to" content such as:
  - Content of extreme/radical nature with violent themes
  - Anarchist Cookbook, explosives or weapons information
  - Military tactics, equipment manuals, chemical or biological information
  - Terrorist/revolutionary literature
  - Preoccupation with press coverage of terrorist attacks
  - Defensive tactics, police or government information
  - Information about timers, electronics, or remote transmitters / receivers

It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different; it does not mean that he or she is suspicious.

Joint Regional Intelligence Center (JRIC)
www.jric.org
(888) 705-JRIC (5742) mention "Tripwire"

What Should I Do?

Be part of the solution.

- ✓ Gather information about individuals without drawing attention to yourself
- ✓ Identify license plates, vehicle description, names used, languages spoken, ethnicity, etc.
- ✓ Do not collect metadata, content, or search electronic communications of individuals
- ✓ Do not do additional logging of on-line activity or monitor communications
- ✓ **If something seems wrong, notify law enforcement authorities.**

Do not jeopardize your safety or the safety of others.

Preventing terrorism is a community effort. By learning what to look for, **you** can make a positive contribution in the fight against terrorism. The **partnership between the community and law enforcement** is essential to the success of anti-terrorism efforts.

Some of the activities, taken individually, could be innocent and must be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. The activities outlined on this handout are by no means all-inclusive but have been compiled from a review of terrorist events over several years.

This project was supported by Grant Number 2007-MU-BX-K002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Each indictor listed above, is by itself, lawful conduct or behavior and may also constitute the exercise of rights guaranteed by the U.S. Constitution. In addition, there may be a wholly innocent explanation for conduct or behavior that appears suspicious in nature. For this reason, no single indicator should be the sole basis for law enforcement action. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

couple of days, use entrances and exits away from the lobby, and stay in their rooms for extended periods of time—none of which seems particularly alarming or even unusual.[16] But at the same time, employees are also being told that finding bags of fertilizer, weapons, explosives, or extremist training manuals in dumpsters or hidden in people's rooms could be a sign of potential terrorist or criminal activity, which does not exactly fall into the "shocking revelation" category.[17]

This kind of juxtaposition between the clearly alarming and the probably innocuous may seem odd, but what it does is create a link in the minds of those reading these fliers between vaguely abnormal behavior and the potential for violent terrorist attack. This attempt to turn anything that seems even slightly out of the ordinary into a cause for concern can also be seen at work in the fliers sent to electronics stores, which warn employees to be on the lookout for anyone who purchases "unusual combinations" of items, such as 2-way radios, GPS technology, infrared devices, police scanners, batteries, wire and soldering tools, night vision equipment, and flashlight bulbs, just to name a few.[18] So basically, people who don't get the chance to go to an electronics store very often and need to buy a lot of different things when they finally have the chance to visit one should now be considered some kind of a threat, and a call to local authorities or a nearby FBI office might very well be in order if this kind of "suspicious activity" has been observed.

At the bottom of its fliers, the FBI reminds the reader that "it is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different, it does not mean that he or she is suspicious."[19] But this nod to political correctness runs completely counter to the actual content of these bulletins, which encourage people to define anything that seems the least bit out of the ordinary as a possible indicator of terrorist intent.

Immunity From Restraint And Common Sense

In its discussion of the "If You See Something, Say Something" initiative on its website, the Department of Homeland Security states the following:

"Factors such as race, ethnicity, national origin, or religious affiliation alone are not suspicious. For that reason, the public should report only suspicious behavior and situations…rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity."[20]

But if the government is really so concerned about preventing false SARs based on bigotry or cultural misunderstanding, why are they taking steps to protect anyone who intentionally makes a false report about supposed terrorist-related activity from ever being held accountable for their actions?

In June of last year, the chairman of the House of Representatives Judiciary Committee, Rep. Lamar Smith (R-TX), introduced the transparently-titled "See Something, Say Something Act of 2011," which would provide

complete immunity from civil liability to anyone who files a false SAR, as well as to the police who investigate those reports.[21] So if your neighbor phones in an SAR accusing you of shouting "Death to America!" while unloading sacks of fertilizer into the back of your truck simply as a way to get back at you for not inviting him to your barbecue, you would not be able to sue him if you ended up getting harassed by law enforcement or if rumors spread around town that you were a secret al-Qaeda operative.

Supposedly this act is designed to provide reassurance to those who might otherwise fear the consequences of getting involved. However, what this piece of legislation will really do if it eventually becomes law is send the message that if you see anything you think *might* be suspicious or threatening, you should just go ahead and report it since you won't have to worry about what will happen if it turns out you are wrong.

So again, it almost seems as if the government *wants* citizens to feel free to indulge their darkest fears and imaginations, even though the onslaught of false suspicious activity reports which this hyper-vigilance will inevitably unleash will presumably negate the effectiveness and accuracy of the NSI database, while also undermining the SAR cause in general. Needless to say, if true, this is curious in the extreme.

The Suspicious Nature Of "Suspicious Activity"

When the Homeland Security Act was being debated back in 2002, plans were made to introduce a citizen surveillance program called the

Operation Terrorism and Prevention System, or Operation TIPS. Originally conceived in the Department of Justice, Operation TIPS was to be a system for collecting and analyzing human intelligence that would give "truckers, letter carriers, train conductors, ship captains, utility employees, and others a formal way to report suspicious [or] potentially terrorist-related activity."[22] Fortunately, many realized a system that turned service providers into roving spies would encourage a degree of invasiveness that would push the Fourth Amendment to the breaking point, and when the Homeland Security Act was finally passed, it specifically excluded this type of initiative.

But the architects of the American surveillance state have shown themselves unwilling to take "no" for an answer. Time and again, when specific ideas or concepts have been rejected for being too intrusive or constitutionally dubious, those same ideas have been brought back again in a different form, and it is easy to see the fingerprints of Operation TIPS in both the "If You See Something, Say Something" and "Communities Against Terrorism" campaigns. The government agencies that are supporting the overall SAR initiative seem bound and determined to foster a climate of distrust where citizens are routinely conflating the truly suspicious with the mundane and at this point, it is hard not to draw the conclusion that this is at least partially intentional.

But if that were the case, the question that of course would have to be asked is, why? What motivation would the government have for inventing a culture of suspicion so hysterical and overwrought that it would inevitably produce an avalanche of useless and misleading data that would undoubtedly hinder rather than help those operating on the frontlines in the war on terror?

One possible explanation is that the attempt to involve the public directly in the search for terrorists is more of a public relations ploy than an actual effort to uncover useful information. Recruiting average American citizens into the war on terror is a way to get them thinking about that war again, at a time when perhaps the public's willingness to accept the gradual erosion of their rights and privileges in the name of greater security has started to wane. Additionally, involving the people themselves in the creation of the surveillance state may be seen as a good way to condition them into becoming used to living in a society where real privacy is destined to become a thing of the past.

In regard to the damage that a lot of false SARs might cause to the government's efforts to protect us from the real terrorist threat, just because tons of suspicious activity reports are being collected from the public and investigated by (mostly) local law enforcement does not

mean that the process is actually being taken all that seriously. In truth, most of the serious action in the construction and operation of the great American surveillance state is now taking place in cyberspace and on the electronic frontier, and despite its value in a normal court of law, eyewitness testimony is probably considered to be little more than a footnote at this point to the greater anti-terror project by those who are running things behind the scenes. Consequently, the SAR initiative could perhaps best be seen as part of a sophisticated marketing campaign designed to convince the American people that the threat of future terrorism is so dire that we should all welcome the arrival of the surveillance state with relief rather than dread.

CHAPTER 2:

THE ELECTRONIC SURVEILLANCE GRID:

LAYING THE FOUNDATIONS

With vulnerability comes opportunity—this is the adage that perhaps best describes the government's apparently insatiable appetite for electronic surveillance and data capture. When digital and wireless technologies began to transform the American communications system, law enforcement officials quickly realized they were facing some new and unique challenges, and that they would have to rapidly adapt if they hoped to stay ahead of the game in the ongoing struggle against organized criminal activities of all types, including potential terrorism.

In response to pressure from the Justice Department, in 1994 Congress passed the Communications Assistance for Law Enforcement Act, which expanded the government's traditional wiretapping privileges to include the wireless networks used by cell phones.[23] The original CALEA mandate required all phone service providers to offer total access to the FBI or any other investigating agency that was able to obtain a court order authorizing a wiretap against a specific human target. But of course, the use of digital technologies for the purposes of communication and information storage has continued to evolve over the course of the past 20 years, and the government's interest in upgrading its capacity to gain access to all the available networks of data has only accelerated at a rate commensurate with this expansion. CALEA, in its initial form, represented a relatively modest beginning to the government's electronic surveillance program, but it proved to be a foreshadowing of things to come.

Surveillance In The Name Of Patriotism

It is entirely possible that the modern American surveillance state may have come into being even if the terrorist attacks of September 11, 2001 had never occurred. But there is no doubt those shocking events galvanized the nation and lit a fire under a government that had been caught unprepared for such an audacious and massive assault. Consequently, a flurry of proposals for how to reshape the U.S. security system were brought together and combined in the 1,000-plus pages of the first Patriot Act, which was passed by both the House and the Senate on October 24, 2001 and signed into law by President Bush on October 26.[24]

Past terrorist investigations of foreign terrorism on American soil had been carried out under the auspices of the Foreign Intelligence and

Surveillance Act of 1978 (FISA). The Patriot Act was based on the recognition that this piece of legislation was sorely in need of improvement and updating, and the new law was designed to close any existing holes in security while expanding and reconfiguring the FISA system in ways that made sense in a context where the nature of the threat had clearly changed.

Some of the sections of the Patriot Act that relate to electronic surveillance and intelligence collection specifically include:[25]

- Sec. 201: Grants authority to government police agencies to intercept wire, oral, and electronic communications relating to terrorism. This provision of the Patriot Act could be seen as the grandfather of the great American surveillance state.
- Sec. 206: Gives roving surveillance authority to agencies carrying out wiretapping operations under the Foreign Intelligence Surveillance Act of 1978. This means that rather than receiving permission to wiretap a specific telephone, authorities are allowed to follow a suspect around, setting up intercepts anywhere it is believed that person may be.
- Sec. 215: Sets out the terms under which access to records and other items can be obtained under the Foreign Intelligence Surveillance Act. If authorized by a FISA court warrant, among the types of documents that can be seized and examined, either in paper form or electronically, are records from banks, Internet companies, libraries, medical clinics, and private businesses of any type.[26]
- Sec. 216: Modification of authorities relating to use of pen registers, and trap and trace devices (wiretapping or communication interceptions that do not require a court order).

The Patriot Act provided a new, more liberalized legal basis for electronic search and surveillance procedures, but with the help of the secretive FISA court system, it appears the government has actually been broadening its mandate beyond what had originally been intended. Two members of the Senate intelligence committee, Ron Wyden (D-OR) and Stewart Udall (D-CO), have begun referring to a second "Secret Patriot Act," apparently in reference to FISA court rulings that are allowing the government to conduct records seizures under Sec. 215 that cannot sensibly be connected to legitimate targets of terrorist investigations.[27] While the secret

nature of FISA proceedings are forcing Wyden and Udall to be somewhat circumspect in their public comments, it appears the government is using the authority granted to them by the Patriot Act to go on fishing expeditions, snooping through the records of even those who have been only tangentially connected to supposed terrorism or criminal suspects, in the hopes that they might find something interesting.

This sort of activity would seem to be in clear violation of the "probable cause" aspect of the Fourth Amendment, which forbids courts from granting warrants for such seizures without evidence of wrongdoing. But FISA courts apparently are not taking the probable cause concept very seriously—according to the latest Justice Department report available under the Freedom of Information Act, in 2010, all 1,506 requests by the government to carry out electronic surveillance-related activities against individuals who may have been somehow aiding foreign powers or terrorist organizations on U.S. soil were approved by the secret FISA judiciary.[28]

If all of these requests had specifically targeted those with obvious connections to terrorism, a statistic like this might not be so alarming. But thanks to the whistle-blowing activity of Wyden and Udall, as well as other anonymous sources with inside knowledge, it has become clear that the government is pushing things far beyond this sensible standard. What revelations show is that the Patriot Act has been used as an excuse to justify a covert expansion of the surveillance state that goes far beyond what had originally been intended. Or, conversely, that those who authored the certain clauses in the legislation knew all along that these sections might give government lawyers enough wiggle room to convince the courts to keep expanding the government's authority indefinitely. It may have been realized that as long as arguments could be made before judicial bodies issuing their rulings in secret, the chances of getting judges to ignore the Constitution for the "greater good" of fighting the war on terror would be dramatically enhanced.

But despite the fluidity of the Patriot Act, the government is not relying on this document alone to justify its ever-growing electronic surveillance and seizure operations. In fact, the Patriot Act was only the beginning.

CHAPTER 3:
THE FBI AND THE NATIONAL ELECTRONIC SURVEILLANCE STRATEGY

Even though certain aspects of the overall program remain shrouded in mystery, the two organizations that appear to be taking the lead in the area of electronic surveillance and data capture are the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). While the NSA tends to operate mostly behind the scenes, FBI and justice department officials have been quite upfront and vocal in expressing their concerns about the way their investigations into criminal activity in general, and potential terrorism in particular, are being obstructed by the rapid advancement of digital and wireless technologies.

It was lobbying from the DOJ and its law enforcement arm that was responsible for the passage of CALEA back in 1994. Over time, the reach of this law has been extended to cover broadband ISPs (Internet service providers) and voice-over Internet companies such as Vonage. But gaining real-time access to modern telephone communications networks has not satisfied the appetite of the FBI for more information about the subjects of their various criminal investigations. Consequently, over the past several years, the country's most well-known police agency has been in the process of developing a comprehensive plan for dramatically expanding its reach into the cyber world, which inside the Bureau is referred to as the National Electronic Surveillance Strategy.

Don't Let The Sun Go Down On Me

Both in private deliberations and in public testimony before Congress, top officials at the FBI have been expressing their concern for some time that the shift of communications from telephone systems to the Internet has the potential to dramatically hinder their ability to carry out effective criminal investigations. In fact, the Bureau has been so worried about this situation that they even made up a catchy title to describe what they claim has been happening—"Going Dark." In 2008, the RAND Commission was contracted to perform an in-depth study of the problem and to make recommendations for change, while in 2010 the FBI set up a Going Dark working group that made itself busy by collecting anecdotes from the field to demonstrate how investigations were hitting brick walls because of the inability of agents to monitor and intercept Internet-based communications.[29]

The primary strategy of the FBI for combating "Going Dark" has been to urge Congress and the White House to change the terms of CALEA at reauthorization in order to keep up with the most recent technological developments. The current proposal for change, which is expected to be sent to Capitol Hill by the Obama administration some time after the next election, would reword this act to require social networking sites,

as well as providers of instant messaging, web email, and VoIP services, to build electronic back doors into their systems that would give FBI agents access to all communications taking place (if approved by court order).[30] It is also believed that the FCC, which is responsible for interpreting CALEA, is now prepared to begin reinterpreting this legislation to apply to video or voice chat services like Skype and Xbox Live, forcing their providers to also grant back door access for wiretapping and surveillance.[31]

Assuming the latest reauthorization is approved—which seems to be little more than a formality—virtually all of the remaining barriers that may have prevented the FBI from listening in on any conversations taking place in the digital realm anywhere in the United States will have been removed. But, of course, they will need to have the technological capacity to take advantage of this access, and here tremendous progress has been made over the past few years. While more work is planned to continue improving their snooping technology, the FBI has already built a highly-advanced super-speedy electronic surveillance system that can establish an instantaneous wiretap on almost every type of electronic communications device imaginable. This system, which is known as the Digital Collection System Network, or DCSNet, can play back recordings as they are captured without delay, create wiretap master files, use cell tower information to track individuals to specific locations, stream intercepted messages to mobile surveillance vans, and send files to translators who are always on standby, ready to provide their services.[32] FBI surveillance rooms are located in field offices and other secret locations across the U.S., and are interconnected through a highly-encrypted network that allows command and control functions to be performed from anywhere up and down the line.[33]

The Domestic Communications Assistance Center

While the FBI's electronic surveillance abilities are quite advanced already, the Bureau remains obsessed with improving their capabilities in order to keep up with enemies whose technological sophistication apparently knows no bounds. In a cooperative venture with the U.S. Marshal's Service and the Drug Enforcement Administration, the FBI has

formed a research and development organization called the Domestic Communication Assistance Center. The mission of this new initiative is two-fold: first, to perfect electronic surveillance technologies so that law enforcement agencies will have the ability to eavesdrop on any kind of Internet, wireless, or VoIP communications, regardless of how well encrypted or otherwise protected they might be; and two, to provide technical assistance to local, state, and federal agencies looking to upgrade their existing surveillance capabilities.[34]

Even beyond the mushrooming complexity of digital communication technologies in general, extremely complicated encryption codes appear to present a unique challenge to FBI code breakers and existing code-breaking software. In 2011, the FBI's general counsel stated in testimony before Congress that the organization's goal was to develop "individually tailored" surveillance solutions that would allow specific individuals or companies to be targeted, and this would mean finding the means to handle even the most clever and intricate efforts to electronically shelter nefarious activity.[35] Encryption is essentially the last bastion of privacy in digital communications, and if the FBI and other government organizations learn how to decode even the most complicated patterns, there will be literally nothing left that will be off-limits from the prying eyes of the agents of the American surveillance state.

Of course, the FBI's interest in achieving such extensive electronic access is supposedly based only on their interest in carrying out court-approved wiretapping operations against criminal suspects, which is something that has already been happening for years. However, in 2008, a whistle-blower who had worked for a major wireless phone carrier (unnamed at the time, but now known to be Verizon) came forward to reveal that the FBI had been given secret, unlimited access to his company's phone system, giving them the ability to monitor customers' voice calls, text messages, billing information, personal data packages, and even their physical movements.[36] None of this was done under the auspices of CALEA, was kept completely secret, and was in fact entirely illegal, which naturally raises suspicions that the FBI is just as interested in going on fishing expeditions as any other agency involved in the creation of the surveillance state. And considering the fact that it is the FBI in particular that has gained a reputation over the years for harassing social activists opposing official government policy, stories like this do not give one confidence that the Bureau will use its soon-to-be unlimited access to the personal communications records of every American wisely or with restraint.

CHAPTER 4:
THE NSA AND THE SUPER-SECRET SURVEILLANCE STATE

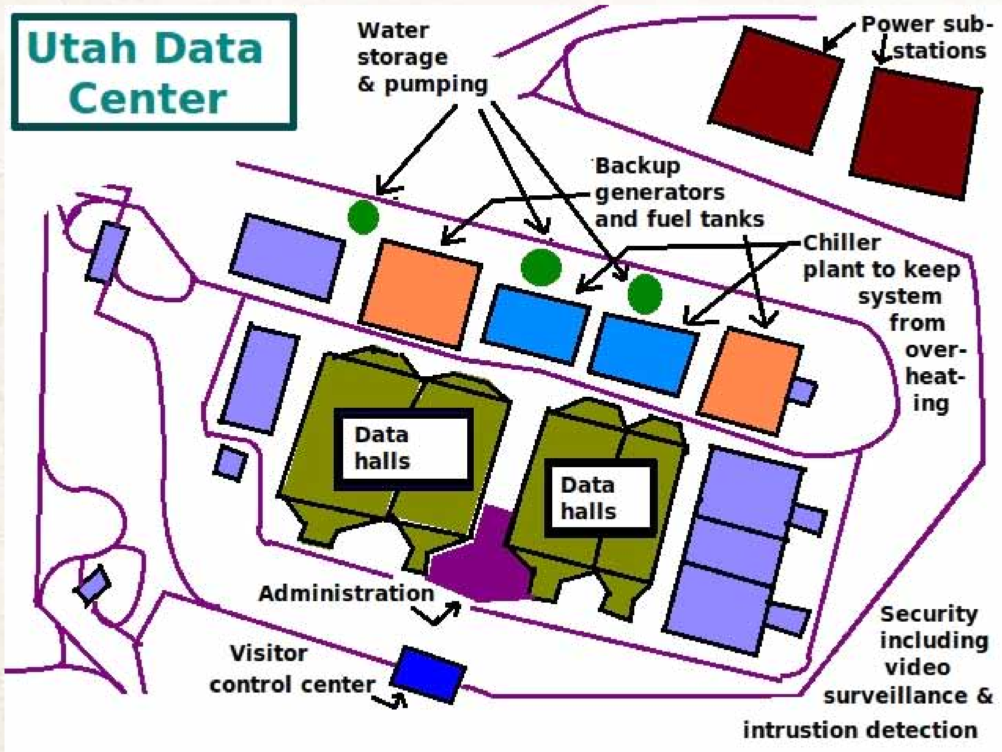
Chapter 4: The NSA And The Super-Secret Surveillance State

Few people really know much about the National Security Agency (NSA), and that is exactly the way the organization likes it. First created in 1952, the NSA has been given a special responsibility to guard the internal security of the United States against any possible foreign threat, and throughout its existence it has been allowed to operate not just in the shadows, but in the shadows of the shadows. The interception and interpretation of foreign communications both on American soil and around the globe is the NSA's specialty. Given this focus, it is hardly surprising that they would be at the center of the attempt to develop a perfectly functioning surveillance state. In the wake of the September 11th terrorist attacks, the NSA has evolved into the largest and most secretive intelligence organization the world has ever seen, and it is now prepared to open a new facility that will truly represent the pièce de résistance of the government's campaign to gain access to every last bit of information they could ever possibly hope to find in the vast reaches of cyberspace and the electronic information network.

The Utah Data Center

In the Utah desert not far outside of Salt Lake City, the innocuously-named $2 billion Utah Data Center is slated to begin operations in September 2013. But when this state-of-the-art information collection and analysis facility finally does have its grand opening, the public most certainly will ***not*** be invited to attend, as this new top secret NSA complex will be nothing less than the largest spying and surveillance center that has ever been constructed anywhere in this solar system.

Located inside the Utah Data Center's heavily-guarded fortress will be supercomputers powerful enough and fast enough to decode, analyze, categorize, and preserve enough information to fill up to one million square feet of data storage space, and these computers will be fed a constant raging river of data as it is being intercepted in real time by a vast network of NSA installations spread far and wide across the continent.[37] Included in this vast warehouse of re-routed data will be the complete contents of private emails, cell phone calls, website visits, search engine inquiries, travel itineraries, library book withdrawal lists, parking receipts, credit card transactions, and a whole hodge-podge of private data that will range from the trivial to the sensitive, to the embarrassing to the actually incriminating in a rare number of cases.[38] And with the amount of storage space and processing power they have available, the NSA could target all 300 million Americans for private data collection and analysis without breaking a sweat.



If things were to stop here, we would be talking about the creation of a collection of data that would be quite extensive indeed. But in reality, the NSA has much bigger fish to fry, and what they are really most interested in is what is referred to as the "deep web." This is all of the sensitive, highly-protected data that is available online but completely hidden from the view of the general public, even though it can be accessed through the Internet by those who know the right paths to follow and the right keywords to enter. Hidden behind convoluted encryption codes, and not accessible through any of the well-known public search engines, this information includes password-protected data of all types, intergovernmental communications taking place within the U.S. and around the world, non-commercial files being shared by trusted peers, and a wealth of classified information held by hostile foreign powers, including details about the sponsorship of terrorism or programs to develop weapons of mass destruction.[39] For an organization that deals in stolen secrets, this is all familiar territory, and anything that enhances the NSA's ability to acquire this type of information would undoubtedly allow it to pursue its primary mission more comprehensively and completely.

But there is much more to the deep web than sensitive information that might embarrass or compromise unfriendly foreign powers. In this highly-encrypted world the most depraved human hearts have found

refuge, and this includes, to quote one source, "drug dealers, arms dealers, hackers, kidnappers, gangs, perverts, assassins, *terrorist networks* [emphasis added], etc."[40] Child pornography is available in abundance on the deep web, along with just about every other kind of horrific activity imaginable, and plenty of advice can be found on how to successfully carry out any type of illegal or criminal act, including how to build bombs.[41]

Overall, the deep web is estimated to contain 7,500 terabytes of information compared to the 19 terabytes of information found in the surface web, and it also has nearly 550 billion documents compared to the one billion that are accessible through the usual public search engines.[42] Theoretically, the new Utah Data Center will allow the NSA to examine and analyze all of this data, and track down anyone involved in any type of illegal activity whatsoever. The decryption software used by the NSA has advanced significantly in recent years, and as part of a technological initiative called the High Productivity Computing Systems Project, NSA computer scientists were able to develop a new type of mega-supercomputer powerful enough to handle and process the avalanche of streaming data that will be captured and diverted by the NSA's network of eavesdropping satellites, domestic listening posts, and secret monitoring rooms located in telecom facilities all across the country.[43]

Stellar Wind: The NSA Throws Its Pole In The Water

Despite its being sanctioned to operate in the shadows, the NSA is still subject to regulation and, like any other law enforcement body of the federal government, it is supposed to gain permission from the FISA court system before proceeding with any investigation that involves targeted electronic surveillance or eavesdropping. But once again, whistle-blowers have revealed a truth that is at odds with this picture of probity and reverence for the due process of law. Shortly after the terrorist attacks of September 11, 2001, the NSA opened up a secret warrantless wiretapping program code named Stellar Wind, which illegally monitored and eavesdropped on the emails and phone calls of untold numbers of Americans, allegedly searching for any kind of needle in a haystack that might indicate a connection to international terrorism.[44] The existence of Stellar Wind, which can now be found listed in any encyclopedia under the category "textbook example of a fishing expedition that violates Fourth Amendment protections," was revealed in 2006 by a former AT&T technician who released internal documents from the company detailing how the NSA had been allowed free reign

to install software that monitored telephone and Internet traffic looking for addresses, names from watch lists, certain keywords or phrases (i.e. bomb, al Qaeda, Death to America!, etc.), and anything else that might be considered incriminating.[45] Anytime something suspicious was found, the call or email in question would then be electronically redirected to NSA headquarters in Fort Meade, Maryland for further analysis.

This reliance on extra-constitutional means to gain information about the activities of the American people is nothing new to the NSA. In Project Minaret, the organization illegally tapped into the phone calls of anti-war protesters during the Vietnam era, while Project Shamrock was a decades-long program that involved the interception and copying of almost every telegram sent inside or into the U.S.—and both of these initiatives were kept completely shielded from congressional oversight.[46] But lest anyone think Congress might be upset at revelations about things like this, the argument that the war on terror justifies anything has an amazing amount of stamina and endurance, which explains why the FISA Act was amended by legislators in 2008 to retroactively legalize everything the NSA had done while at the same time granting immunity from prosecution to the ISPs and the giant telecommunications firms that had cooperated with Stellar Wind.[47]

According to another whistle-blower who left the NSA shortly after Stellar Wind began, the NSA's approach to fighting terrorism is all about unrestricted and unfiltered data mining. In other words, they will be using the vast computing and decoding capacities of the new Utah Data Center to look through every single bit of information they can get their hands on, from wherever they can find it. And, because this new spying facility will be so top secret, oversight will be all but nonexistent. In the words of one NSA official who spoke off the record about the organization's plans for the American people going forward: "Everybody's a target; everybody with communication is a target."[48]

CHAPTER 5:
DOMESTIC DRONES AND THE ALL-SEEING EYE IN THE SKY

With neighbors watching neighbors and cyber-spies monitoring everyone's digital activities, it would seem the designers of the American surveillance state already have us all enmeshed in a very sticky spider's web. But just to make sure that no one is safe from the all-seeing eye of the state, there is one last step being taken to ensure that our every movement can be tracked and monitored.

Even though the two-way telescreen of "1984" Oceania has not yet been developed, the government has managed to come up with the next best thing. If they cannot see what everyone is doing in the privacy of their own homes, at least they will be able to see what we are up to whenever we step outside of our doors. This is all thanks to the coming deployment of total visual surveillance technology in the form of unmanned aerial vehicles (UAVs), more commonly known as drones. While domestic drones with highly advanced visual surveillance capabilities are not yet commonplace, that situation is expected to change dramatically over the next eight years, as the Federal Aviation Administration (FAA) is predicting that at least 30,000 unmanned aerial vehicles will be regularly patrolling our airspace by the year 2020.[49]

Domesticating A Killer

Unmanned aerial vehicles are remote-controlled quasi-airplanes that do not require an onboard pilot. Using the most advanced aerodynamic principles, these flying machines come in a variety of shapes and sizes (most domestic drones will be smaller than a single-engine airplane), but the one thing they all have in common is they can be flown and maneuvered with perfect precision from far-off locations. Drones were originally developed for use by the military as a way to deliver deadly payloads or find dangerous enemies without putting pilots in harm's way. However, because they can be so easily outfitted with high-resolution cameras and infrared sensors, it quickly became apparent after their invention that drones could be used quite effectively for a variety of law enforcement and security-related purposes.

When furnished with sophisticated and sensitive onboard electronic equipment, drones can deliver detailed and highly accurate pictures of everything that appears on the ground beneath them, including any human being who might be engaged in some sort of suspicious activity. The first organization to effectively demonstrate the usefulness of surveillance drones for non-military purposes on American soil was an affiliate of the Department of Homeland Security called the U.S. Customs and Border Protection, which operates ten drones along the U.S.-Mexican

border that are being used primarily to help detect narcotics smuggling activity.[50] But a few law enforcement agencies and departments have now purchased drones for use in various capacities related to criminal surveillance, and while the number of drones being used for these purposes in the U.S. is still fairly small, the FAA did issue 313 certificates to government and police agencies in 2011 authorizing drone flights in U.S. airspace.[51]

In response to the enthusiasm of police departments all across the country for this technology, in February 2012, Congress passed the Federal Aviation Administration Air Transportation Modernization and Safety Improvement Act, which will require the FAA to:

a. Develop an expedited process for the approval of drone flights by federal, state, and local entities before the end of the calendar year.

b. Facilitate the military's use of civilian airspace for drone flights over certain areas of the country.

c. Set up a system for the authorization of commercial drone use by the year 2015.

d. Fully integrate drones into the U.S. National Airspace System within a three-year period.[52]

Estimates of the cost for a small UAV outfitted with appropriate equipment for surveillance are in the $30,000 - $50,000 range, which would be

similar to what it would cost a local or state police department to purchase a brand new squad car.[53] So far, a total of 12 state and local law enforcement agencies have received FAA approval to fly drones, but this number is expected to climb significantly in the coming years as the cost efficiency and safety advantages of this technology becomes more readily apparent.[54] Besides its basic utility for reconnaissance, patrol, and search-and-rescue missions, drones could save lives by providing vital on-site information to police departments before men and women are actually sent in to make arrests or resolve potential conflicts.

But once again, we must be prepared for the possibility, (or more, the likelihood), that police departments will use drones to go on fishing expeditions, discreetly peeking at anyone and everyone without anything remotely resembling probable cause. As the technologies of surveillance get more advanced, domestic drones may be able to zoom in and spy on people right through their windows, which would give police the kind of secret access to private activity previously enjoyed only by James Stewart's character in the Hitchcock classic Rear Window. And drones operated by commercial or private interests would be able to spy on people at will, without any checks and balances whatsoever, since anything recorded by their cameras would presumably be protected from search or seizure. But of course, if so-called commercial interests are allowed to fly drones in U.S. airspace with impunity, there will be nothing to stop rogue government agencies (are there any other kind, really?) from using private organizations as a front for top-secret surveillance missions that will be completely protected from any kind of control or oversight.

Biometric Tracking And The Future Of Drones

In order to improve their ability to track specific individuals from the air, the military has been funding research into the use of biometrics for tracking. Biometric systems allow for the identification of individuals based on physical traits or characteristics that can be picked up through visual or infrared monitoring, facilitating effective tracking of targeted persons from a distance. Working under a military contract, a company called Progeny has developed something called the "Long Range, Non-cooperative Biometric Tagging, Tracking and Location" system, which will allow precise three-dimensional images of faces to be constructed from two-dimensional photographs.[55] Progeny claims that just 50 photographic pixels taken of a target's face, in the area between the eyes, will be enough to generate an accurate 3-D profile, and that only 15-20 pixels will be required to identify a person once an original facial recreation has been entered into databanks.[56] Additionally, for those times when facial recognition is not possible, the Progeny system will still allow individuals to be tracked and monitored by making use of so-called "soft biometrics"—skin color, age, gender, height, weight, etc.[57]

While the development of biometric tracking is impressive, a company called Charles Rive Analytics is taking things to the next level. This research-and-development firm has created an amazing new system for the Army called the "Adversary Behavior Acquisition, Collection, Understanding, and Summarization (ABACUS)" tool.[58] This program would feed information gained from informant's tips, eavesdropping operations, and drone surveillance into a human behavior modeling-and-simulation engine which would then be able to generate an "intent-based threat assessments of individuals and/or groups."[59] In other words, the ABACUS tool would be able to predict specific types of future behavior based on past patterns of behavior. Or to put it in still another way, ABACUS will essentially be able to read minds.

Meanwhile, on the home front, the Department of Homeland Security has started to experiment with a program called Future Attribute Screening Technology, or FAST, which relies on remote sensors to detect physiological indicators of "malintent" such as elevated heart rate, rapid eye movements, fidgeting, and so on.[60] So if you are standing in a long line at the airport, for example, and you start to get nervous or uncomfortable, FAST technology will spot your discomfort, and you may soon find yourself being pulled aside for a private interview by a friendly agent of the TSA.

A group photo of aerial demonstrators at the 2005 Naval Unmanned Aerial Vehicle Air Demo.

Many psychologists and psychiatrists who study human behavior and consciousness dismiss attempts to read minds and uncover intentions through programs like ABACUS and FAST as little more than pseudo-science. Nevertheless, the government is apparently determined to leave no stone unturned in its search for ways to root out arch-criminals and terrorists, and if that means delving into the realm of the fantastic or the quasi-scientific, then so be it.

There is little doubt that biometric tracking capabilities, modeling-and-simulation software, and remote physiological sensing equipment of the most sophisticated type will all be installed on domestic drones at some point. But if the trained behavioral experts are right, and a part of the drone surveillance package will be operating on principles that are the technological equivalent of reading tea leaves, then it is inevitable that many innocent people who seem to be behaving "suspiciously" will face intense scrutiny and possibly extensive harassment from authorities who are convinced that they must be up to no good.

Armed And Dangerous

Once drones become a fixture over the skies of America, federal, state, and local law enforcement authorities will have significantly increased

their ability to monitor our patterns of behavior when we are out in public. If some police officials have their way, however, these drones may be able to do more than just watch us. In an announcement that caught the attention of many, Chief Deputy Randy McDaniel of the Montgomery County (Texas) Sheriff's Office recently stated that his department would like to outfit any drones they purchase with rubber bullets and tear gas, which could be remotely used to help break up riots, subdue out-of-control suspects, or perform a number of other services that would normally require police officers to be present on the scene.[61]

If one high-ranking officer in one police department is saying this publicly, we can be sure that other law enforcement agencies are also thinking that it would be a wonderful idea to arm their drones too. Police enthusiasm for such a thing aside, however, it should be obvious to just about everyone that if law enforcement agencies are given the power to start relying on remote-controlled violence to stop civil disobedience or any other type of allegedly criminal activity, the temptation to use that violence indiscriminately will undoubtedly prove to be all but irresistible.

Shoot First, Ask Questions Later

But this is how it is with virtually all of the initiatives and technologies associated with the implementation of the American surveillance state. Because of their intrinsically hidden and intrusive natures, the potential for misuse and abuse will be strong, and past history gives us no reason to be comforted by the facile reassurances of law enforcement and intelligence agencies that they will respect the privacy of innocent people while solemnly upholding the sanctity of the Constitution. The problem is that the organizers of the surveillance state, whether they are willing to admit it or not, are planning to treat us all as if we are guilty until proven innocent—they may not know exactly what it is we are guilty of, but they will operate under the assumption that it must be something. And because their surveillance methods are so well-hidden, we will have no way to defend ourselves from their misinterpretations of our words or actions—or even realize that we need to defend ourselves, until that day comes when they actually show up at our doors to ask us some questions.

But of course, if they start arming drones, they may not even have to bother showing up at our doors at all.

CONCLUSION:

PERVASIVE SURVEILLANCE AND THE FRAMEWORK OF TOTALITARIANISM

Conclusion: Pervasive Surveillance And The Framework Of Totalitarianism

In 2003, the Pentagon's Office of Information Awareness, under the direction of the notorious John Poindexter of Iran-Contra fame, introduced a new program called Total Information Awareness. In the words of Poindexter, the idea was to "break down the stovepipes" that separate government and commercial databases so that his organization could then gain access to the personal information of the majority of the American people, including such things as credit card purchases, travel itineraries, medical histories, financial reports, email accounts, telephone records, Internet purchases, and so on.[62]

When word of this plan leaked out, the outrage of the general public, among legislators, and in the media about such an unwarranted (figuratively and literally) invasion of privacy was so strong that Congress explicitly banned this initiative. When you carefully examine everything that has been happening over the past few years, however, it quickly becomes apparent that the federal law enforcement and intelligence establishment has been gradually and stealthily instituting this very same program, only without using the actual name. And perhaps even more disturbingly, they have been doing so with the full cooperation of most members of Congress and the last two presidential administrations.

While the era of Total Information Awareness is continuing to unfold, the one thing that has changed is that terrorism is no longer the only justification being used to rationalize and explain the creation of the perfect surveillance state. Because there have been no more serious foreign terrorist attacks on U.S. soil since 9/11, the public's enthusiasm for surrendering their rights to help catch terrorists has waned considerably, and therefore it has been necessary to find new reasons to explain the need for more intensive and invasive security measures. Two recent pieces of legislation, one currently being debated in the Congress and one already signed into law by President Obama under the principle of executive privilege, reveal some of the new strategies that are being tried out by the promoters of the perfect surveillance society.

As an unacknowledged companion to his earlier-discussed "See Something, Say Something Act," our old friend Rep. Lamar Smith (R-TX) has also introduced a bill to the House of Representatives called the "Protecting Children from Internet Pornographers Act of 2011."[63] Supposedly designed to stop sinister predators from preying on our children (and who could possibly be opposed to that?), this bill would require every single ISP, as well as any other company providing

"electronic communications" or "remote computing" services, to keep track of all activity taking place on any IP address or other type of Internet access they provide.[64] If required to do so by a U.S. Marshal Service subpoena, these companies must be prepared to provide a complete record of any customer's Internet activity over the previous 18 months, including data about search engine queries, social networking activity, downloads, methods of payment for services, and website visits.[65] To issue these subpoenas, the Marshal's Service only has to claim that it has something to do with a child porn investigation and the courts will back them to the hilt.

The second significant piece of legislation worth mentioning is the international Anti-Counterfeiting Trade Agreement, recently signed into law by President Obama under executive privilege, without the approval of Congress.[66] This legislation is designed to prevent copyrighted material from being used online without permission, by anyone, and it will impose potentially significant penalties on anyone caught violating the rules. The important point with this legislation is that ISPs will be held liable for copyright infringements in addition to offenders, so the only way for Internet companies to protect themselves will be—you guessed it—to maintain comprehensive records on the Internet activity of all their users to make sure no violations of these new ironclad anti-intellectual property theft laws are occurring.

When we step back to take a look at the bigger picture, it becomes crystal clear that whatever the justification the government decides to use, they are absolutely determined to create a society where the concept of personal privacy is relegated to a footnote in history. The war on terror, the war on child porn, and the war on copyright infringement only exist to provide the rationale for elevating the interests of the surveillance state above any constitutional principles that might interfere with the government's unquenchable desire to know everything about everyone.

The people behind the creation of the surveillance state may honestly believe that what they are doing will serve the greater good, and that even if it tramples on the Fourth Amendment a bit, it will all be worth it in the end. But as the English statesman Lord Acton observed, "Power tends to corrupt, and absolute power corrupts absolutely."[67] If power is defined as being accountable to no one or having the ability to abuse authority with impunity while escaping detection, then there is little doubt that those in charge of the great American surveillance state do in fact hold immense power, which under the right circumstances could devolve into the absolute.

The Party in Orwell's Oceania no doubt started out with good intentions before they got lost in their own rhetoric and descended into the pit of tyranny. But that is how the road to hell is paved, as they say, and when you set up a framework in which totalitarianism has the potential to flourish, no one should be surprised if, at some point, that is exactly what happens.

Notes

1 http://www.online-literature.com/orwell/1984/2/

2 http://www.napoleonguide.com/revolt.htm

3 http://www.nytimes.com/2007/08/30/us/30jewell.html

4 http://www.law.cornell.edu/constitution/fourth_amendment/

5 http://nsi.ncirc.gov/about_nsi.aspx

6 http://nsi.ncirc.gov/about_nsi.aspx

7 http://nsi.ncirc.gov/documents/NSI_Overview.pdf

8 http://nsi.ncirc.gov/about_nsi.aspx

9 http://nsi.ncirc.gov/about_nsi.aspx

10 http://publicintelligence.net/fusion-center-locations-revealed/

11 http://www.dhs.gov/ynews/releases/pr_1303758062431.shtm

12 http://newmexicoindependent.com/68938/is-dhs%E2%80%99s-%E2%80%98if-you-see-something-say-something%E2%80%99-campaign-helpful-or-burden-some

13 http://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/

14 http://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/

15 http://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/

16 http://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/

17 http://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/

18 http://www.networkworld.com/community/blog/25-more-ridiculous-fbi-lists-you-might-be-terrorist-if

19 http://publicintelligence.net/fbi-suspicious-activity-reporting-flyers/

20 http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm

21 http://politicalcorrection.org/blog/201106230009

22 http://www.villagevoice.com/2002-12-17/news/the-death-of-operation-tips/1/

23 http://www.wired.com/threatlevel/2008/03/whistleblower-f/

24 http://www.historycommons.org/context.jsp?item=a102601patriotact

25 http://w2.eff.org/Censorship/Terrorism_militias/hr3162.php

26 http://www.wired.com/threatlevel/2012/03/declassify-spy-court-rulings/

27 http://www.wired.com/dangerroom/2011/05/secret-patriot-act/

28 http://www.wired.com/threatlevel/2012/03/declassify-spy-court-rulings/

29 http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/?tag=mncol;txt

30 http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/?tag=mncol;txt

31 http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/?tag=mncol;txt

32 http://www.wired.com/politics/security/news/2007/08/wiretap?currentPage=all

33 http://www.wired.com/politics/security/news/2007/08/wiretap?currentPage=all

34 http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit/

35 http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit/

36 http://www.wired.com/threatlevel/2008/03/whistleblower-f/

37 http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

38 http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

39 http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

40 http://www.acceleratedstudynotes.com/2012/02/17/accessing-deep-web/

41 http://thenewsjunkie.com/2011/06/inside-the-deep-web-my-journey-through-the-new-underground/

42 http://www.acceleratedstudynotes.com/2012/02/17/accessing-deep-web/

43 http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

44 http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

45 http://www.globalresearch.ca/index.php?context=va&aid=30079

46 http://www.globalresearch.ca/index.php?context=va&aid=30079

47 http://www.telepresenceoptions.com/2012/04/nsa_chief_denies_domestic_spyi/

48 http://www.globalresearch.ca/index.php?context=va&aid=30079

49 http://www.washingtontimes.com/news/2012/feb/7/coming-to-a-sky-near-you/?page=2

50 http://cnsnews.com/news/article/faa-has-authorized-106-government-entities-fly-domestic-drones

51 http://www.washingtontimes.com/news/2012/feb/7/coming-to-a-sky-near-you/?page=2

52 http://www.washingtontimes.com/news/2012/feb/7/coming-to-a-sky-near-you/?page=2

53 http://cnsnews.com/news/article/faa-has-authorized-106-government-entities-fly-domestic-drones

54 http://cnsnews.com/news/article/faa-has-authorized-106-government-entities-fly-domestic-drones

55 http://www.sott.net/articles/show/235564-Army-Developing-Drones-That-Can-Recognize-Your-Face-From-a-Distance

56 http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face/

57 http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face/

58 http://www.sott.net/articles/show/235564-Army-Developing-Drones-That-Can-Recognize-Your-Face-From-a-Distance

59 http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face/

60 http://www.nature.com/news/2011/110527/full/news.2011.323.html

61 http://washington.cbslocal.com/2012/05/23/groups-concerned-over-arming-of-domestic-drones/

62 http://www.cato.org/publications/commentary/beware-total-information-awareness

63 http://www.itworld.com/security/251584/sopa-replacement-uses-child-porn-excuse-spy-997-percent-americans

64 http://www.itworld.com/security/251584/sopa-replacement-uses-child-porn-excuse-spy-997-percent-americans

65 http://www.itworld.com/security/251584/sopa-replacement-uses-child-porn-excuse-spy-997-percent-americans

66 http://endthelie.com/2012/01/27/acta-the-legislation-that-makes-sopa-and-pipa-look-reasonable/#axzz1zrgYBIw9

67 http://www.quotationspage.com/quote/27321.html