# NO PLACE TO HIDE

EDWARD SNOWDEN, THE NSA, AND THE U. S. SURVEILLANCE STATE

GLENN GREENWALD

2014

METROPOLITAN BOOKS HENRY HOLT NEW YORK

4

# THE HARM OF SURVEILLANCE

Governments around the world have made vigorous attempts to train citizens to disdain their own privacy. A litany of now-familiar platitudes has convinced people to tolerate severe encroachments into their private realm; so successful are these justifications that many people applaud as the authorities collect vast amounts of data about what they say, read, buy, and do—and with whom.

Those state authorities have been assisted in their assault on privacy by a chorus of Internet moguls—the government's indispensable partners in surveillance. When Google CEO Eric Schmidt was asked in a 2009 CNBC interview about concerns over his company's retention of user data, he infamously replied: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." With equal dismissiveness, Facebook founder and CEO Mark Zuckerberg said in a 2010 interview that "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people." Privacy in the digital age is no longer a "social norm," he claimed, a notion that handily serves the interests of a tech company trading on personal information.

But the importance of privacy is evident in the fact that even those who devalue it, who have declared it dead or dispensable, do not be-

lieve the things they say. Anti-privacy advocates have often gone to great lengths to maintain control over the visibility of their own behavior and information. The US government itself has used extreme measures to shield its actions from public view, erecting an ever-higher wall of secrecy behind which it operates. As a 2011 report from the ACLU argued, "Today much of our government's business is conducted in secret." So secretive is this shadowy world, "so large, so unwieldy," as the *Washington Post* reported, that no one knows how much money it costs, how many people it employs, how many programs exist within it or exactly how many agencies do the same work."

Similarly, those Internet tycoons who are so willing to devalue our privacy are vehemently protective of their own. Google insisted on a policy of not talking to reporters from CNET, the technology news site, after CNET published Eric Schmidt's personal details—including his salary, campaign donations, and address, all public information obtained via Google—in order to highlight the invasive dangers of his company.

Meanwhile, Mark Zuckerberg purchased the four homes adjacent to his own in Palo Alto, at a cost of $30 million, to ensure his privacy. As CNET put it, "Your personal life is now known as Facebook's data. Its CEO's personal life is now known as mind your own business."

The same contradiction is expressed by the many ordinary citizens who dismiss the value of privacy yet nonetheless have passwords on their email and social media accounts. They put locks on their bathroom doors; they seal the envelopes containing their letters. They engage in conduct when nobody is watching that they would never consider when acting in full view. They say things to friends, psychologists, and lawyers that they do not want anyone else to know. They give voice to thoughts online that they do not want associated with their names.

The many pro-surveillance advocates I have debated since Snowden blew the whistle have been quick to echo Eric Schmidt's view that privacy is for people who have something to hide. But none of them would willingly give me the passwords to their email accounts, or allow video cameras in their homes.

When the Senate Intelligence Committee's chair, Dianne Feinstein, insisted that the NSA's collection of metadata does not con-

stitute surveillance—because it does not include the content of any communication—online protesters demanded that she back up her assertion with action: Would the senator, each month, publish a full list of people she emailed and called, including the length of time they spoke and their physical locations when the call was made? That she would take up the offer was inconceivable precisely because such information is profoundly revealing; making it public would constitute a true breach of one's private realm.

The point is not the hypocrisy of those who disparage the value of privacy while intensely safeguarding their own, although that is striking. It is that the desire for privacy is shared by us all as an essential, not ancillary, part of what it means to be human. We all instinctively understand that the private realm is where we can act, think, speak, write, experiment, and choose how to be, away from the judgmental eyes of others. Privacy is a core condition of being a free person.

Perhaps the most famous formulation of what privacy means and why it is so universally and supremely desired was offered by US Supreme Court Justice Louis Brandeis in the 1928 case *Olmstead v. U.S.*: "The right to be left alone [is] the most comprehensive of rights, and the right most valued by a free people." The value of privacy, he wrote, "is much broader in scope" than mere civic freedoms. It is, he said, fundamental:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone.

Even before Brandeis was appointed to the Court, he was an ardent proponent of the importance of privacy. Together with lawyer Samuel Warren, he wrote the seminal 1890 *Harvard Law Review* article "The Right to Privacy," arguing that robbing someone of their privacy was a crime of a deeply different nature than the theft of a material belonging.

"The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality."

Privacy is essential to human freedom and happiness for reasons that are rarely discussed but instinctively understood by most people, as evidenced by the lengths to which they go to protect their own. To begin with, people radically change their behavior when they know they are being watched. They will strive to do that which is expected of them. They want to avoid shame and condemnation. They do so by adhering tightly to accepted social practices, by staying within imposed boundaries, avoiding action that might be seen as deviant or abnormal.

The range of choices people consider when they believe that others are watching is therefore far more limited than what they might do when acting in a private realm. A denial of privacy operates to severely restrict one's freedom of choice.

Several years ago, I attended the bat mitzvah of my best friend's daughter. During the ceremony, the rabbi emphasized that "the central lesson" for the girl to learn was that she was "always being watched and judged." He told her that God always knew what she was doing, every choice, every action, and even every thought, no matter how private. "You are never alone," he said, which meant that she should always adhere to God's will.

The rabbi's point was clear: if you can never evade the watchful eyes of a supreme authority, there is no choice but to follow the dictates that authority imposes. You cannot even consider forging your own path beyond those rules: if you believe you are always being watched and judged, you are not really a free individual.

All oppressive authorities—political, religious, societal, parental—rely on this vital truth, using it as a principal tool to enforce orthodoxies, compel adherence, and quash dissent. It is in their interest to convey that nothing their subjects do will escape the knowledge of the authorities. Far more effectively than a police force, the deprivation of privacy will crush any temptation to deviate from rules and norms.

What is lost when the private realm is abolished are many of the at-

tributes typically associated with quality of life. Most people have experienced how privacy enables liberation from constraint. And we've all, conversely, had the experience of engaging in private behavior when we thought we were alone—dancing, confessing, exploring sexual expression, sharing untested ideas—only to feel shame at having been seen by others.

Only when we believe that nobody else is watching us do we feel free—safe—to truly experiment, to test boundaries, to explore new ways of thinking and being, to explore what it means to be ourselves. What made the Internet so appealing was precisely that it afforded the ability to speak and act anonymously, which is so vital to individual exploration.

For that reason, it is in the realm of privacy where creativity, dissent, and challenges to orthodoxy germinate. A society in which everyone knows they can be watched by the state—where the private realm is effectively eliminated—is one in which those attributes are lost, at both the societal and the individual level.

Mass surveillance by the state is therefore inherently repressive, even in the unlikely case that it is not abused by vindictive officials to do things like gain private information about political opponents. Regardless of how surveillance is used or abused, the limits it imposes on freedom are intrinsic to its existence.

Invoking George Orwell's *1984* is something of a cliché, but the echoes of the world about which he warned in the NSA's surveillance state are unmistakable: both rely on the existence of a technological system with the capacity to monitor every citizen's actions and words. The similarity is denied by the surveillance champions—we're not *always* being watched, they say—but that argument misses the point. In *1984*, citizens were not necessarily monitored at all times; in fact, they had no idea whether they were ever actually being monitored. But the state had the capability to watch them at any time. It was the uncertainty and possibility of ubiquitous surveillance that served to keep everyone in line:

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

Even the NSA, with its capacity, could not read every email, listen to every telephone call, and track the actions of each individual. What makes a surveillance system effective in controlling human behavior is the knowledge that one's words and actions are susceptible to monitoring.

This principle was at the heart of British philosopher Jeremy Bentham's eighteenth-century conception of the Panopticon, a building design he believed would allow institutions to effectively control human behavior. The building's structure was to be used, in his words, for "any sort of establishment, in which persons of any description are to be kept under inspection." The Panopticon's primary architectural innovation was a large central tower from which every room—or cell, or classroom, or ward—could be monitored at any time by guards. The inhabitants, however, were not able to see into the tower and so could never know whether they were or were not being watched.

Since the institution—any institution—was not capable of observing all of the people all of the time, Bentham's solution was to create "the apparent omnipresence of the inspector" in the minds of the inhabitants. "The persons to be inspected should always feel themselves as if under inspection, at least as standing a great chance of being so." They would thus act as if they were always being watched, even if they weren't. The result would be compliance, obedience, and conformity with expectations.

Bentham envisioned that his creation would spread far beyond prisons and mental hospitals to all societal institutions. Inculcating in the minds of citizens that they might always be monitored would, he understood, revolutionize human behavior.

In the 1970s, Michel Foucault observed that the principle of Bentham's Panopticon was one of the foundational mechanisms of the modern state. In *Power*, he wrote that Panopticonism is "a type of power that is applied to individuals in the form of continuous individual supervision, in the form of control, punishment, and compensation, and in the form of correction, that is, the moulding and transformation of individuals in terms of certain norms."

In *Discipline and Punish*, Foucault further explained that ubiquitous surveillance not only empowers authorities and compels compliance but also induces individuals to internalize their watchers. Those who believe they are watched will instinctively choose to do that which is wanted of them without even realizing that they are being controlled—the Panopticon induces "in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power." With the control internalized, the overt evidence of repression disappears because it is no longer necessary: "the external power may throw off its physical weight; it tends to be non-corporal; and, the more it approaches this limit, the more constant, profound and permanent are its effects: it is a profound victory that avoids any physical confrontation and which is always decided in advance."

Additionally, this model of control has the great advantage of simultaneously creating the illusion of freedom. The compulsion to obedience exists in the individual's mind. Individuals choose on their own to comply, out of fear that they are being watched. That eliminates the need for all the visible hallmarks of compulsion, and thus enables control over people who falsely believe themselves to be free.

For this reason, every oppressive state views mass surveillance as one of its most critical instruments of control. When the normally restrained German chancellor Angela Merkel learned that the NSA had spent years eavesdropping on her personal cell phone, she spoke to President Obama and angrily likened US surveillance to the Stasi, the notorious security

service of East Germany, where she grew up. Merkel did not mean that the United States was the equivalent of the Communist regime; rather that the essence of a menacing surveillance state, be it the NSA or the Stasi or Big Brother or the Panopticon, is the knowledge that one can be watched at any time by unseen authorities.

It is not hard to understand why authorities in the United States and other Western nations have been tempted to construct a ubiquitous system of spying directed at their own citizens. Worsening economic inequality, converted into a full-blown crisis by the financial collapse in 2008, has generated grave internal instability. There has been visible unrest even in relatively stable democracies, such as Spain and Greece. In 2011, there were days of rioting in London. In the United States both the Right—the Tea Party protests of 2008 and 2009—and the Left—the Occupy movement—have launched enduring citizens protests. Polls in these countries revealed strikingly intense levels of discontent with the political class and direction of society.

Authorities faced with unrest generally have two options: to placate the population with symbolic concessions or fortify their control to minimize the harm it can do their interests. Elites in the West seem to view the second option—fortifying their power—as their better, perhaps only viable course of action to protect their position. The response to the Occupy movement was to crush it with force, through tear gas, pepper spray, and prosecution. The para-militarization of domestic police forces was on full display in American cities, as police officers brought out weapons seen on the streets of Baghdad to quell legally assembled and largely peaceful protesters. The strategy was to put people in fear of attending marches and protests, and it generally worked. The more general aim was to cultivate the sense that this sort of resistance is futile against a massive and impenetrable establishment force.

A system of ubiquitous surveillance achieves the same goal but with even greater potency. Merely organizing movements of dissent becomes difficult when the government is watching everything people are doing. But mass surveillance kills dissent in a deeper and more important place

as well: in the mind, where the individual trains him- or herself to think only in line with what is expected and demanded.

History leaves no doubt that collective coercion and control is both the intent and effect of state surveillance. The Hollywood screenwriter Walter Bernstein, who was blacklisted and monitored during the McCarthy era, forced to write under pseudonyms to continue working, has described the dynamic of oppressive self-censorship that comes from the sense of being watched:

> Everybody was careful. It was not a time for risk taking. . . . There were writers, non-blacklisted writers who did, I don't know what you'd call them, "cutting-edge things," but not political. They stayed away from politics. . . . I think there was a general feeling of "You don't stick your neck out."
>
> It's not an atmosphere that helps creativity or lets the mind run free. You're always in danger of self-censorship, of saying "no, I won't try this because I know it's not going to get done or it'll alienate the government," or something like that.

Bernstein's observations were eerily echoed in a report released by PEN America in November 2013 entitled *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*. The organization conducted a survey to look at the effects of the NSA revelations on its members, finding that many writers now "assume that their communications are being monitored" and have changed their behavior in ways that "curtail their freedom of expression and restrict the free flow of information." Specifically, "24% have deliberately avoided certain topics in phone or email conversations."

The pernicious controlling power of ubiquitous surveillance and the self-censorship that results are confirmed in a range of social science experiments and extend far beyond political activism. Ample studies show how this dynamic works at the deepest personal and psychological levels.

One team of researchers, publishing their findings in the journal *Evolutionary Psychology*, presented their subjects with morally questionable

actions, such as keeping a sizeable amount of money found in a wallet on the street or knowing that a friend had added false information to his résumé. The subjects were asked to assess the degree of wrongdoing. The study noted that subjects who were shown images hinting at surveillance, such as a large pair of staring eyes, rated the actions as more "reprehensible" than those who were shown a neutral image. The researchers concluded that surveillance encourages those who are being watched to "affirm their endorsement of prevailing social norms" as they attempt to "actively manage their reputations."

A comprehensive experiment conducted in 1975 by Stanford University psychologists Gregory White and Philip Zimbardo, entitled "The Chilling Effects of Surveillance," sought to assess whether being watched had an impact on the expression of controversial political opinions. The impetus for the study was Americans' concerns about surveillance by the government:

> The Watergate scandal, revelations of White House bugging, and Congressional investigations of domestic spying by the Central Intelligence Agency have served to underscore the developing paranoid theme of American life: Big Brother may be watching you! Proposals for national data banks, uses of surveillance helicopters by urban police forces, the presence of observation cameras in banks and supermarkets, and airport security searches of person and property are but some of the signs that our private lives are under such increasing scrutiny.

The participants were placed under varying levels of surveillance and asked to give their views on the legalization of marijuana.

It turned out that "threatened" subjects—those who were told that their statements would be shared with the police "for training purposes"—were more likely to condemn marijuana usage and to use second- and third-person pronouns ("you," "they," "people") in their language. Only 44 percent of subjects under surveillance advocated for legalization, compared to 77 percent of those not so "threatened." Tellingly, 31 percent of the participants being monitored spontaneously sought approval from the researchers (asking, for example, "Is that all

right?"), whereas only 7 percent of the other group did so. Participants who were "threatened" also scored significantly higher on feelings of anxiety and inhibition.

White and Zimbardo noted in their conclusion that the "threat or actuality of government surveillance may psychologically inhibit freedom of speech." They added that while their "research design did not allow for the possibility of 'avoiding assembly,'" they expected that "the anxiety generated by the threat of surveillance would cause many people to totally avoid situations" in which they might be monitored. "Since such assumptions are limited only by one's imagination and are encouraged daily by revelations of government and institutional invasion of privacy," they wrote, "the boundaries between paranoid delusions and justified cautions indeed become tenuous."

It is true that surveillance can at times promote what some may consider desirable behavior. One study found that rowdiness in Swedish soccer stadiums—fans throwing bottles and lighters onto the field—declined by 65 percent after the introduction of security cameras. And public health literature on hand washing has repeatedly confirmed that the way to increase the likelihood of someone washing his or her hands is to put someone nearby.

But overwhelmingly, the effect of being watched is to severely constrain individual choice. Even in the most intimate of settings, within the family, for example, surveillance turns insignificant actions into a source of self-judgment and anxiety, just by virtue of being observed. In one UK experiment, researchers provided subjects with tracking devices to keep tabs on family members. Any member's precise location was accessible at any time, and if someone's location had been viewed, he would receive a message. Each time one member tracked another, he was also sent a questionnaire asking why he had done so and whether the information received had matched expectations.

In the debriefing, participants said that while they sometimes found the tracking comforting, they also felt anxious that if they were in an unexpected place, family members would "jump to conclusions" about their behavior. And the option of "going invisible"—blocking the location-sharing mechanism—did not resolve the anxiety: many participants

said that the act of avoiding surveillance in and of itself would generate suspicion. The researchers concluded:

> There are trails in our daily life that we cannot explain and that may be completely insignificant. However, their representation via a tracking device . . . gives them significance, seemingly calling for an extraordinary degree of accountability. This generates anxieties, especially within close relationships, in which people may feel under greater pressure to account for things they simply cannot account for.

For a Finnish experiment that carried out one of the most radical simulations of surveillance, cameras were placed in subjects' homes—bathrooms and bedrooms excluded—and all of their electronic communications were tracked. Although the advertisement for the study went viral on social media, the researchers had difficulty getting even ten households to participate.

Among those who signed up, complaints about the project focused on the invasion of ordinary parts of their daily lives. One person felt uncomfortable being naked in her home; another felt conscious of the cameras while fixing her hair after a shower; someone else thought of the surveillance while injecting medicine. Innocuous actions gained layers of significance when surveilled.

Subjects initially described the surveillance as annoying; however, they soon "got used to it." What began as deeply invasive became normalized, transformed into the usual state of affairs and no longer noticed.

As the experiments showed, there are all sorts of things people do that they are eager to keep private, even though these sorts of things do not constitute doing "something wrong." Privacy is indispensable to a wide range of human activities. If someone calls a suicide hotline or visits an abortion provider or frequents an online sex website or makes an appointment with a rehabilitation clinic or is treated for a disease, or if a whistle-blower calls a reporter, there are many reasons for keeping such acts private that have no connection to illegality or wrongdoing.

In sum, everyone has something to hide. Reporter Barton Gellman made the point this way:

> Privacy is relational. It depends on your audience. You don't want your employer to know you're job hunting. You don't spill all about your love life to your mom, or your kids. You don't tell trade secrets to your rivals. We don't expose ourselves indiscriminately and we care enough about exposure to lie as a matter of course. Among upstanding citizens, researchers have consistently found that lying is "an everyday social interaction" (twice a day among college students, once a day in the Real World). . . . Comprehensive transparency is a nightmare. . . . Everyone has something to hide.

A prime justification for surveillance—that it's for the benefit of the population—relies on projecting a view of the world that divides citizens into categories of good people and bad people. In that view, the authorities use their surveillance powers only against bad people, those who are "doing something wrong," and only they have anything to fear from the invasion of their privacy. This is an old tactic. In a 1969 *Time* magazine article about Americans' growing concerns over the US government's surveillance powers, Nixon's attorney general, John Mitchell, assured readers that "any citizen of the United States who is not involved in some illegal activity has nothing to fear whatsoever."

The point was made again by a White House spokesman, responding to the 2005 controversy over Bush's illegal eavesdropping program: "This is not about monitoring phone calls designed to arrange Little League practice or what to bring to a potluck dinner. These are designed to monitor calls from very bad people to very bad people." And when President Obama appeared on *The Tonight Show* in August 2013 and was asked by Jay Leno about NSA revelations, he said: "We don't have a domestic spying program. What we do have is some mechanisms that can track a phone number or an email address that is connected to a terrorist attack."

For many, the argument works. The perception that invasive surveillance is confined only to a marginalized and deserving group of those "doing wrong"—the bad people—ensures that the majority acquiesces to the abuse of power or even cheers it on.

But that view radically misunderstands what goals drive all institu-

tions of authority. "Doing something wrong," in the eyes of such institutions, encompasses far more than illegal acts, violent behavior, and terrorist plots. It typically extends to meaningful dissent and any genuine challenge. It is the nature of authority to equate dissent with wrongdoing, or at least with a threat.

The record is suffused with examples of groups and individuals being placed under government surveillance by virtue of their dissenting views and activism—Martin Luther King, the civil rights movement, antiwar activists, environmentalists. In the eyes of the government and J. Edgar Hoover's FBI, they were all "doing something wrong": political activity that threatened the prevailing order.

Nobody understood better than Hoover the power of surveillance to crush political dissent, confronted as he was with the challenge of how to prevent the exercise of First Amendment rights of speech and association when the state is barred from arresting people for expressing unpopular views. The 1960s ushered in a slew of Supreme Court cases that established rigorous protections for free speech, culminating in the unanimous 1969 decision in *Brandenburg v. Ohio*, which overturned the criminal conviction of a Ku Klux Klan leader who had threatened violence against political officials in a speech. The Court said that the First Amendment guarantees of free speech and free press are so strong that they "do not permit a State to forbid or proscribe advocacy of the use of force."

Given those guarantees, Hoover instituted a system to prevent dissent from developing in the first place.

The FBI's domestic counterintelligence program, COINTELPRO, was first exposed by a group of antiwar activists who had become convinced that the antiwar movement had been infiltrated, placed under surveillance, and targeted with all sorts of dirty tricks. Lacking documentary evidence to prove it and unsuccessful in convincing journalists to write about their suspicions, they broke into an FBI branch office in Pennsylvania in 1971 and carted off thousands of documents.

Files related to COINTELPRO showed how the FBI had targeted political groups and individuals it deemed subversive and dangerous, including the National Association for the Advancement of Colored

People, black nationalist movements, socialist and Communist organizations, antiwar protesters, and various right-wing groups. The bureau had infiltrated them with agents who, among other things, attempted to manipulate members into agreeing to commit criminal acts so that the FBI could arrest and prosecute them.

The FBI succeeded in convincing the *New York Times* to suppress the documents and even return them, but the *Washington Post* published a series of articles based on them. Those revelations led to the creation of the Senate Church Committee, which concluded:

> [Over the course of fifteen years] the Bureau conducted a sophisticated vigilate operation aimed squarely at preventing the exercise of First Amendment rights of speech and association, on the theory that preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence.
>
> Many of the techniques used woud be intolerable in a democratic society even if all of the targets had been involved in violent activity, but COINTELPRO went far beyond that. The unexpressed major premise of the programs was that a law enforcement agency has the duty to do whatever is necessary to combat perceived threats to the existing social and political order.

One key COINTELPRO memo explained that "paranoia" could be sown among antiwar activists by letting them believe there was "an F.B.I. agent behind every mailbox." In this way, dissidents, always convinced that they were being watched, would drown in fear and refrain from activism.

Unsurprisingly, the tactic worked. In a 2013 documentary entitled *1971*, several of the activists described how Hoover's FBI was "all over" the civil rights movement with infiltrators and surveillance, people who came to meetings and reported back. The monitoring impeded the movement's ability to organize and grow.

At the time, even the most entrenched institutions in Washington understood that the mere existence of government surveillance, no matter how it is used, stifles the ability to dissent. The *Washington Post*, in a

March 1975 editorial on the break-in, warned about precisely this oppressive dynamic:

> The FBI has never shown much sensitivity to the poisonous effect which its surveillance, and especially its reliance on faceless informers, has upon the democratic process and upon the practice of free speech. But it must be self-evident that discussion and controversy respecting governmental policies and programs are bound to be inhibited if it is known that Big Brother, under disguise, is listening to them and reporting them.

COINTELPRO was far from the only surveillance abuse found by the Church Committee. Its final report declared that "millions of private telegrams sent from, to, or through the United States were obtained by the National Security Agency from 1947 to 1975 under a secret arrangement with three United States telegraph companies." Moreover, "some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups" during one CIA operation, CHAOS (1967–1973).

Additionally, "an estimated 100,000 Americans were the subjects of United States Army intelligence files created between the mid-1960's and 1971" as well as some 11,000 individuals and groups who were investigated by the Internal Revenue Service "on the basis of political rather than tax criteria." The bureau also used wiretapping to discover vulnerabilities, such as sexual activity, which were then deployed to "neutralize" their targets.

These incidents were not aberrations of the era. During the Bush years, for example, documents obtained by the ACLU revealed, as the group put it in 2006, "new details of Pentagon surveillance of Americans opposed to the Iraq war, including Quakers and student groups." The Pentagon was "keeping tabs on non-violent protestors by collecting information and storing it in a military anti-terrorism database." The ACLU noted that one document, "labeled 'potential terrorist activity,' lists events such as a 'Stop the War NOW!' rally in Akron, Ohio."

The evidence shows that assurances that surveillance is only targeted at those who "have done something wrong" should provide little

comfort, since a state will reflexively view any challenge to its power as wrongdoing.

The opportunity those in power have to characterize political opponents as "national security threats" or even "terrorists" has repeatedly proven irresistible. In the last decade, the government, in an echo of Hoover's FBI, has formally so designated environmental activists, broad swaths of antigovernment right-wing groups, antiwar activists, and associations organized around Palestinian rights. Some individuals within those broad categories may deserve the designation, but undoubtedly most do not, guilty only of holding opposing political views. Yet such groups are routinely targeted for surveillance by the NSA and its partners.

Indeed, after British authorities detained my partner, David Miranda, at Heathrow airport under an antiterrorism statute, the UK government expressly equated my surveillance reporting with terrorism on the ground that the release of the Snowden documents "is designed to influence a government and is made for the purposes of promoting a political or ideological cause. This therefore falls within the definition of terrorism." This is the clearest possible statement of linking a threat to the interests of power to terrorism.

None of this would come as any surprise to the American Muslim community, where the fear of surveillance on the grounds of terrorism is intense and pervasive, and for good reason. In 2012, Adam Goldman and Matt Apuzzo of the Associated Press exposed a joint CIA/New York Police Department scheme of subjecting entire Muslim communities in the United States to physical and electronic surveillance without the slightest whiff of any suggestion of wrongdoing. American Muslims routinely describe the effect of spying on their lives: each new person who shows up at a mosque is regarded with suspicion as an FBI informant; friends and family stifle their conversations for fear of being monitored and out of awareness that any expressed view deemed hostile to America can be used as a pretext for investigation or even prosecution.

One document from the Snowden files, dated October 3, 2012, chillingly underscores the point. It revealed that the agency has been moni-

toring the online activities of individuals it believes express "radical" ideas and who have a "radicalizing" influence on others. The memo discusses six individuals in particular, all Muslims, though it stresses that they are merely "exemplars."

The NSA explicitly states that none of the targeted individuals is a member of a terrorist organization or involved in any terror plots. Instead, their crime is the views they express, which are deemed "radical," a term that warrants pervasive surveillance and destructive campaigns to "exploit vulnerabilities."

Among the information collected about the individuals, at least one of whom is a "U.S. person," are details of their online sex activities and "online promiscuity"—the porn sites they visit and surreptitious sex chats with women who are not their wives. The agency discusses ways to exploit this information to destroy their reputations and credibility.

BACKGROUND (U)

(TS//SI//REL TO USA, FVEY) A previous SIGINT assessment report on radicalization indicated that radicalizers appear to be particularly vulnerable in the area of authority when their private and public behaviors are not consistent. (A) Some of the vulnerabilities, if exposed, would likely call into question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of his authority. Examples of some of these vulnerabilities include:

- Viewing sexually explicit material online or using sexually explicit persuasive language when communicating with inexperienced young girls;
- Using a portion of the donations they are receiving from the susceptible pool to defray their own personal expenses;
- Charging an exorbitant amount of money for their speaking fees and being singularly attracted by opportunities to increase their stature; or
- Being known to base their public messaging on questionable sources or using language that is contradictory in nature, leaving them open to credibility challenges.

(TS//SI//REL TO USA, FVEY) Issues of trust and reputation are important when considering the validity and appeal of the message. It stands to reason that exploiting vulnerabilities of character, credibility, or both, of the radicalizer and his message could be enhanced by an understanding of the vehicles he uses to disseminate his message to the susceptible pool of people and where he is vulnerable in terms of access.

As the ACLU's deputy legal director, Jameel Jaffer, observed, the NSA databases "store information about your political views, your medical history, your intimate relationships and your activities online." The agency claims this personal information won't be abused, "but these docu-

ments show that the NSA probably defines 'abuse' very narrowly." As Jaffer pointed out, the NSA has historically, at a president's request, "used the fruits of surveillance to discredit a political opponent, journalist, or human rights activist." It would be "naive," he said, to think the agency couldn't still "use its power that way."

Other documents describe the government's focus not only on WikiLeaks and its founder, Julian Assange, but also on what the agency calls "the human network that supports WikiLeaks." In August 2010 the Obama administration urged several allies to file criminal charges against Assange for the group's publication of the Afghanistan war logs. The discussion around pressuring other nations to prosecute Assange appears in an NSA file that the agency calls its "Manhunting Timeline." It details, on a country-by-country basis, the efforts by the United States and its allies to locate, prosecute, capture, and/or kill various individuals, among them alleged terrorists, drug traffickers, and Palestinian leaders. A timeline exists for each year between 2008 and 2012.

## (U) Manhunting Timeline 2010

**TOP SECRET//SI/TK//NOFORN**

Jump to: navigation, search

*Main article: Manhunting*

*See also: Manhunting Timeline 2011*
*See also: Manhunting Timeline 2009*
*See also: Manhunting Timeline 2008*

**(U) The following manhunting operations took place in Calendar Year 2010:**

### [edit] (U) November

**Contents**

**[edit] (U) United States, Australia, Great Britain, Germany, Iceland**

(U) The United States on 10 August urged other nations with forces in Afghanistan, including Australia, United Kingdom, and Germany, to consider filing criminal charges against Julian Assange, founder of the rogue Wikileaks [internet website and responsible for the unauthorized publication of over 70,000 classified documents covering the war in Afghanistan. The documents may have been provided to Wikileaks by Army Private First Class Bradley Manning. The appeal exemplifies the start of an international effort to focus the legal element of national power upon non-state actor Assange, and the human network that supports Wikileaks.[16]

A separate document contains a summary of a July 2011 exchange regarding whether WikiLeaks, as well as the file-sharing website Pirate

Bay, could be designated as "a 'malicious foreign actor' for the purposes of targeting." The designation would allow extensive electronic surveillance of those websites, including US users. The discussion appears in a running list of "Q&As" in which officials from the NTOC Oversight and Compliance office (NOC) and NSA's Office of General Counsel (OGC) provide answers to submitted questions.

**[edit] (TS//SI//REL) Malicious foreign actor = disseminator of US data?**

**Can we treat a foreign server who stores, or potentially disseminates leaked or stolen US data on it's server as a 'malicious foreign actor' for the purpose of targeting with no defeats? Examples: WikiLeaks, thepiratebay.org, etc.**

NOC/OGC RESPONSE: Let us get back to you. (Source #001)

One such exchange, from 2011, showed the NSA's indifference to breaking the surveillance rules. In the document, an operator says, "I screwed up," having targeted a US person instead of a foreigner. The response from the NSA's oversight office and general counsel is, "it's nothing to worry about."

**[edit] (TS//SI//REL) Unknowingly targeting a US person**

**I screwed up...the selector had a strong indication of being foreign, but it turned out to be US...now what?**

NOC/OGC RESPONSE: With all querying, if you discover it actually is US, then it must be submitted and go in the OGC quarterly report...'but it's nothing to worry about'. (Source #001)

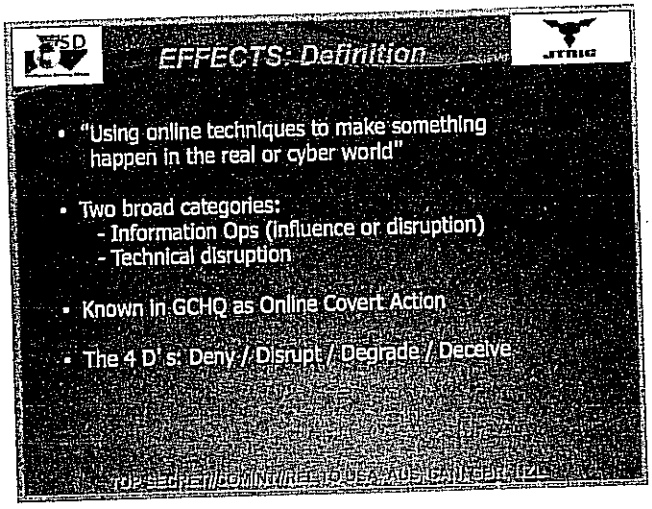
The treatment of Anonymous, as well as the vague category of people known as "hacktivists," is especially troubling and extreme. That's because Anonymous is not actually a structured group but a loosely organized affiliation of people around an idea: someone becomes affiliated with Anonymous by virtue of the positions they hold. Worse still, the category "hacktivists" has no fixed meaning: it can mean the use of programming skills to undermine the security and functioning of the Internet but can also refer to anyone who uses online tools to promote political ideals. That the NSA targets such broad categories of people is

tantamount to allowing it to spy on anyone anywhere, including in the United States, whose ideas the government finds threatening.

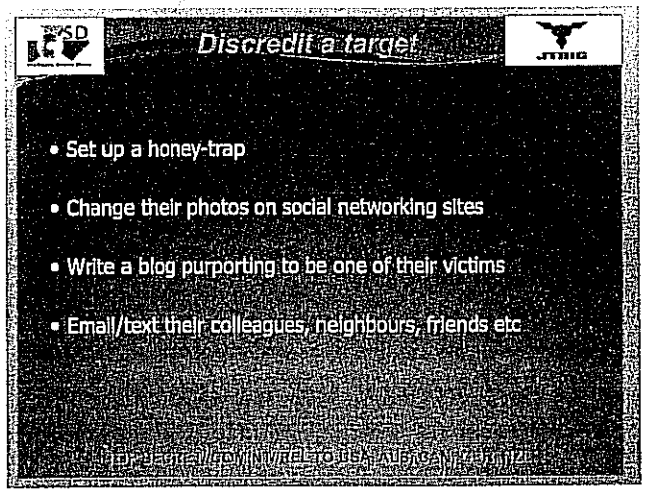
Gabriella Coleman, a specialist on Anonymous at McGill University, said that the group "is not a defined" entity but rather "an idea that mobilizes activists to take collective action and voice political discontent. It is a broad-based global social movement with no centralized or official organized leadership structure. Some have rallied around the name to engage in digital civil disobedience, but nothing remotely resembling terrorism." The majority who have embraced the idea have done so "primarily for ordinary political expression. Targeting Anonymous and hacktivists amounts to targeting citizens for expressing their political beliefs, resulting in the stifling of legitimate dissent," Coleman explained.

Yet Anonymous has been targeted by a unit of the GCHQ that employs some of the most controversial and radical tactics known to spycraft: "false flag operations," "honey-traps," viruses and other attacks, strategies of deception, and "info ops to damage reputations."

One PowerPoint slide presented by GCHQ surveillance officials at the 2012 SigDev conference describes two forms of attack: "information ops (influence or disruption)" and "technical disruption." GCHQ refers to these measures as "Online Covert Action," which is intended to achieve what the document calls "The 4 D's: Deny/Disrupt/Degrade/Deceive."



Another slide describes the tactics used to "discredit a target." These include "set up a honey-trap," "change their photos on social networking sites," "write a blog purporting to be one of their victims," and "email/text their colleagues, neighbors, friends, etc."




In accompanying notes, the GCHQ explains that the "honey trap"—an old Cold War tactic involving using attractive women to lure male targets into compromising, discrediting situations—has been updated for the digital age: now a target is lured to a compromising site or online encounter. The comment added: "a great option. Very successful when it works." Similarly, traditional methods of group infiltration are now accomplished online:

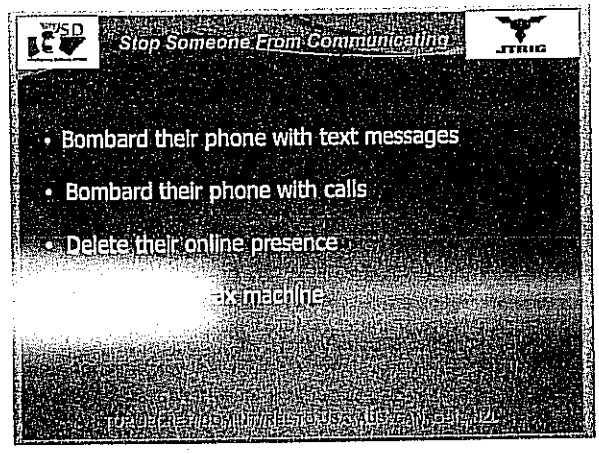
CK

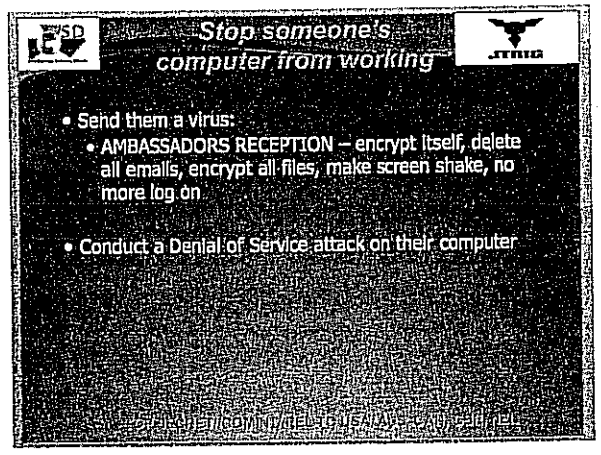
Honey-trap; a great option. Very successful when it works.
- Get someone to go somewhere on the internet, or a physical location to be met by a "friendly face".
- JTRIG has the ability to "shape" the environment on occasions.

Photo change; you have been warned, "JTRIG is about!"
Can take "paranoia" to a whole new level.

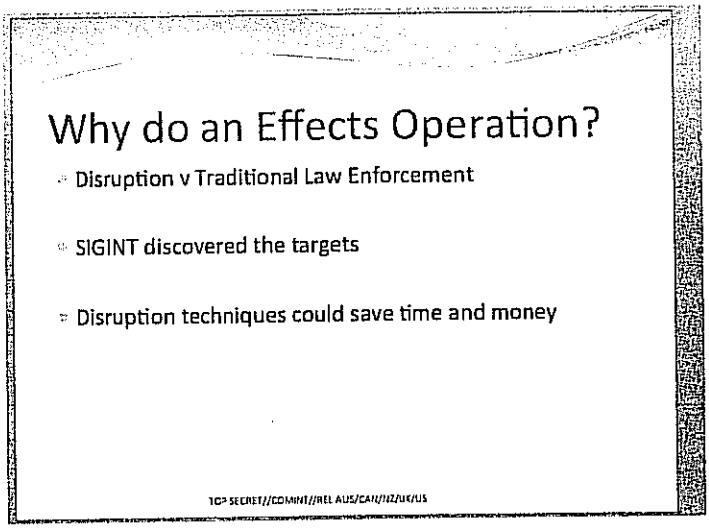
Email/text:
- Infiltration work.
- Helps JTRIG acquire credibility with online groups etc.
- Helps with bringing SIGINT/Effects together.

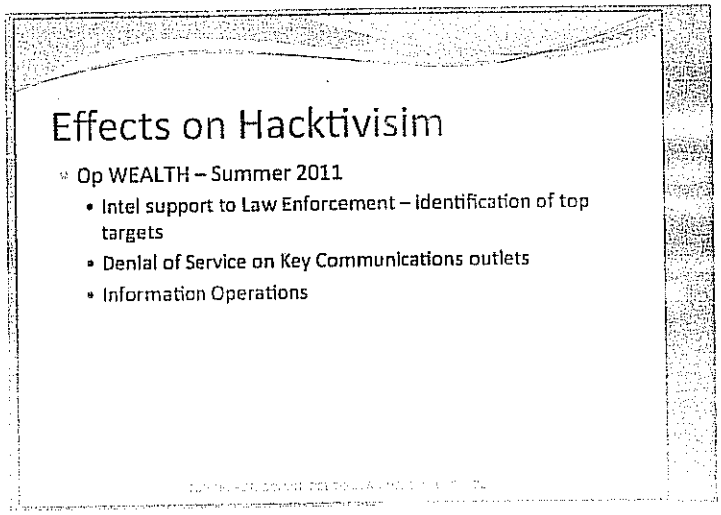
Another technique involves stopping "someone from communicating." To do that, the agency will "bombard their phone with text messages," "bombard their phone with calls," "delete their online presence," and "block up their fax machine."




The GCHQ also likes to use "disruption" techniques in lieu of what it calls "traditional law enforcement" such as evidence-gathering, courts, and prosecutions. In a document entitled "Cyber Offensive Session: Pushing the Boundaries and Action Against Hacktivism," the GCHQ discusses its targeting of "hacktivists" with, ironically, "denial of service" attacks, a tactic commonly associated with hackers:



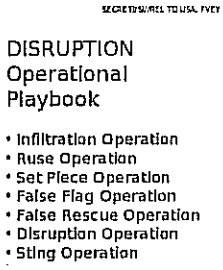




The British surveillance agency also uses a team of social scientists, including psychologists, to develop techniques of "online HUMINT" (human intelligence) and "strategic influence disruption." The document "The Art of Deception: Training for a New Generation of Online Covert Operations" is devoted to these tactics. Prepared by the agency's HSOC (Human Science Operation Cell), the paper claims to draw on sociology, psychology, anthropology, neuroscience, and biology, among other fields, to maximize the GCHQ's online deception skills.

One slide shows how to engage in "Dissimulation—Hide the Real," while propagating "Simulation—Show the False." It examines "the psychological building blocks of deception" and the "map of technologies" used to carry out the deceptions, including Facebook, Twitter, LinkedIn, and "Web Pages."

Emphasizing that "people make decisions for emotional reasons not rational ones," the GCHQ contends that online behavior is driven by "mirroring" ("people copy each other while in social interaction with them"), "accommodation," and "mimicry" ("adoption of specific social traits by the communicator from the other participant").

The document then lays out what it calls the "Disruption Operational Playbook." This includes "infiltration operation," "ruse operation," "false flag operation," and "sting operation." It vows a "full roll out" of the disruption program "by early 2013" as "150+ staff [are] fully trained."


SECRET//REL TO USA, FVEY

DISRUPTION
Operational
Playbook

- Infiltration Operation
- Ruse Operation
- Set Piece Operation
- False Flag Operation
- False Rescue Operation
- Disruption Operation
- Sting Operation

Under the title "Magic Techniques & Experiment," the document references "Legitimisation of violence," "Constructing experience in mind of targets which should be accepted so they don't realize," and "Optimising deception channels."

Such government plans to monitor and influence Internet communications and disseminate false information online have long been a source of speculation. Harvard law professor Cass Sunstein, a close Obama adviser, the White House's former head of the Office of Information and Regulatory Affairs, and an appointee to the White House panel to review NSA activities, wrote a controversial paper in 2008 proposing that the US government employ teams of covert agents and pseudo-"independent" advocates for "cognitive infiltration" of online groups, chat rooms, social networks, and websites, as well as off-line activist groups.

These GCHQ documents show for the first time that these controversial techniques to deceive and harm reputations have moved from the proposal stage to implementation.

All of the evidence highlights the implicit bargain that is offered to citizens: pose no challenge and you have nothing to worry about. Mind your own business, and support or at least tolerate what we do, and you'll be fine. Put differently, you must refrain from provoking the authority that wields surveillance powers if you wish to be deemed free of wrongdoing. This is a deal that invites passivity, obedience, and conformity. The safest course, the way to ensure being "left alone," is to remain quiet, unthreatening, and compliant.

For many, the deal is an attractive one, persuading the majority that surveillance is benign or even beneficial. They are too boring to attract the government's attention, they reason. "I seriously doubt that the NSA is interested in me" is the sort of thing I've often heard. "If they want to listen to my boring life, then they're welcome." Or "the NSA isn't interested in your grandmother talking about her recipes or your dad planning his golf game."

These are people who have become convinced that they themselves are not going to be personally targeted—because they are unthreatening and compliant—and therefore either deny that it's happening, do not care, or are willing to support it outright.

Interviewing me soon after the NSA story broke, MSNBC host Lawrence O'Donnell mocked the notion of the NSA as "a big, scary surveillance monster." Summing up his view, he concluded:

> My feeling so far is . . . I'm not scared . . . the fact that the government is collecting [data] at such a gigantic, massive level means that it's even harder for the government to find me . . . and they have absolutely no incentive to find me. And so I, at this stage, feel completely unthreatened by this.

The *New Yorker*'s Hendrik Hertzberg also asserted similarly dismissive views of the dangers of surveillance. Conceding that there "are reasons

to be concerned about intelligence-agency overreach, excessive secrecy, and lack of transparency," he wrote that "there are also reasons to remain calm," in particular, that the threat posed "to civil liberties, such as it is, is abstract, conjectural, unspecified." And the *Washington Post*'s columnist Ruth Marcus, belittling concern over NSA powers, announced—absurdly—"my metadata almost certainly hasn't been scrutinized."

In one important sense, O'Donnell, Hertzberg, and Marcus are right. It is the case that the US government "has absolutely no incentive" to target people like them, for whom the threat from a surveillance state is little more than "abstract, conjectural, unspecified." That's because journalists who devote their careers to venerating the country's most powerful official—the president, who is the NSA's commander-in-chief—and defending his political party rarely, if ever, risk alienating those in power.

Of course, dutiful, loyal supporters of the president and his policies, good citizens who do nothing to attract negative attention from the powerful, have no reason to fear the surveillance state. This is the case in every society: those who pose no challenge are rarely targeted by oppressive measures, and from their perspective, they can then convince themselves that oppression does not really exist. But the true measure of a society's freedom is how it treats its dissidents and other marginalized groups, not how it treats good loyalists. Even in the world's worst tyrannies, dutiful supporters are immunized from abuses of state power. In Mubarak's Egypt, it was those who took to the street to agitate for his overthrow who were arrested, tortured, gunned down; Mubarak's supporters and people who quietly stayed at home were not. In the United States, it was NAACP leaders, Communists, and civil rights and anti-war activists who were targeted with Hoover's surveillance, not well-behaved citizens who stayed mute about social injustice.

We shouldn't have to be faithful loyalists of the powerful to feel safe from state surveillance. Nor should the price of immunity be refraining from controversial or provocative dissent. We shouldn't want a society where the message is conveyed that you will be left alone only if you mimic the accommodating behavior and conventional wisdom of an establishment columnist.

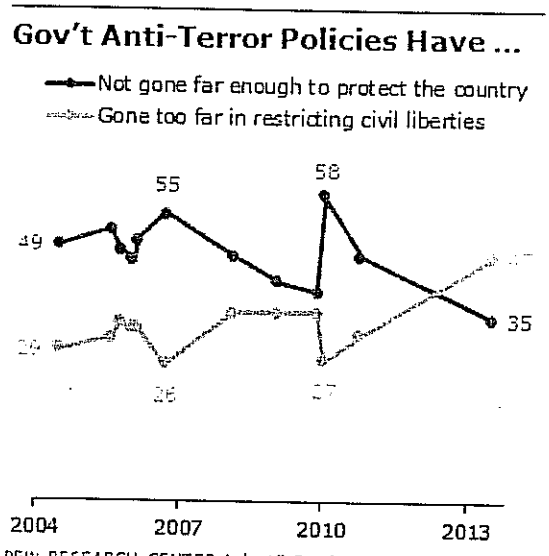
Beyond that, the sense of immunity felt by a particular group currently in power is bound to be illusory. That is made clear when we look at how partisan affiliation shapes people's sense of the dangers of state surveillance. What emerges is that yesterday's cheerleaders can quickly become today's dissenters.

At the time of the 2005 NSA warrantless eavesdropping controversy, liberals and Democrats overwhelmingly viewed the agency's surveillance program as menacing. Part of this, of course, was typical partisan hackery: George W. Bush was president and Democrats saw an opportunity to inflict political harm on him and his party. But a significant part of their fear was genuine: because they considered Bush malicious and dangerous, they perceived that state surveillance under his control was therefore threatening and that they in particular were endangered as political opponents. Accordingly, Republicans had a more benign or supportive view of the NSA's actions. In December 2013, by contrast, Democrats and progressives had converted to the leading NSA defenders.

Ample polling data reflected this shift. At the end of July 2013, the Pew Research Center released a poll showing that the majority of Americans disbelieved the defenses offered for the NSA's actions. In particular, "a majority of Americans—56%—say that federal courts fail to provide adequate limits on the telephone and Internet data the government is collecting as part of its anti-terrorism efforts." And "an even larger percentage (70%) believes that the government uses this data for purposes other than investigating terrorism." Moreover, "63% think the government is also gathering information about the content of communications."

Most remarkably, Americans now considered the danger of surveillance of greater concern than the danger of terrorism:

> Overall, 47% say their greater concern about government anti-terrorism policies is that they have gone too far in restricting the average person's civil liberties, while 35% say they are more concerned that policies have not gone far enough to protect the country. This is the first time in Pew Research polling that more have expressed concern over civil liberties than protection from terrorism since the question was first asked in 2004.




That polling data was good news for anyone alarmed by use of excessive government power and the chronic exaggeration of the threat of terrorism. But it highlighted a telling inversion: Republicans, who had been defenders of the NSA under Bush, had been supplanted by Democrats once the surveillance system had come under the control of President Obama, one of their own. "Nationwide, there is more support for the government's data-collection program among Democrats (57% approve) than among Republicans (44%)."

Similar polling data from the *Washington Post* revealed that conservatives were far more concerned about NSA spying than liberals. When asked, "How concerned are you, if at all, about the collection and use of your personal information by the National Security Agency?" 48 percent of conservatives were "very concerned" compared to only 26 percent of liberals. As law professor Orin Kerr noted, this represented a fundamental change: "It's an interesting reversal from 2006, when the President was a Republican instead of a Democrat. Back then, a Pew poll found 75% of Republicans approved of NSA surveillance but only 37% of Democrats approved."

A Pew chart makes the shift clear:

## Partisan Shifts in Views of NSA Surveillance Programs

Views of NSA surveillance programs
(See previous table for differences in question wording)

| | January 2006 | | June 2013 | |
|---|---|---|---|---|
| | Acceptable % | Unacceptable % | Acceptable % | Unacceptable % |
| Total | 51 | 47 | 56 | 41 |
| Republican | 75 | 23 | 52 | 47 |
| Democrat | 37 | 61 | 64 | 34 |
| Independent | 44 | 55 | 53 | 44 |

PEW RESEARCH CENTER June 6-9, 2013. Figures read across. Don't know/Refused responses not shown.

The arguments for and against surveillance brazenly rotate, based on which party in power. The NSA's collection of bulk metadata was vehemently denounced by one senator on *The Early Show* in 2006 in this way:

> I don't have to listen to your phone calls to know what you're doing. If I know every single phone call that you made, I am able to determine every single person you talked to. I can get a pattern about your life that is very, very intrusive. . . . And the real question here is: What do they do with this information that they collect that does not have anything to do with Al Qaeda? . . . And we're going to trust the president and the vice president of the United States that they're doing the right thing? Don't count me in on that.

The senator so harshly attacking metadata collection was Joe Biden, who subsequently, as vice president, became part of a Democratic administration that advanced precisely the same arguments he once derided.

The relevant point here is not merely that many partisan loyalists are unprincipled hypocrites with no real convictions other than a quest for power, although that is certainly true. More important is what such statements reveal about the nature of how one regards state surveillance. As

with so many injustices, people are willing to dismiss fear of government overreach when they believe that those who happen to be in control are benevolent and trustworthy. They consider surveillance dangerous or worth caring about only when they perceive that they themselves are threatened by it.

Radical expansions of power are often introduced in this way, by persuading people that they affect just a specific, discrete group. Governments have long convinced populations to turn a blind eye to oppressive conduct by leading citizens to believe, rightly or wrongly, that only certain marginalized people are targeted, and everyone else can acquiesce to or even support that oppression without fear that it will be applied to them. Leaving aside the obvious moral shortcomings of this position—we do not dismiss racism because it is directed at a minority, or shrug off hunger on the grounds that we enjoy a plentiful supply of food—it is almost always misguided on pragmatic grounds.

The indifference or support of those who think themselves exempt invariably allows for the misuse of power to spread far beyond its original application, until the abuse becomes impossible to control—as it inevitably will. There are too many examples to count, but perhaps the most recent and potent one is the exploitation of the Patriot Act. A near-unanimous Congress approved a massive increase in surveillance and detention powers after 9/11, convinced by the argument that doing so would detect and prevent future attacks.

The implicit assumption was that the powers would be used principally against Muslims in relation to terrorism—a classic expansion of power confined to a particular group engaged in a particular kind of act—which is one reason why the measure received overwhelming backing. But what happened was very different: the Patriot Act has been applied well beyond its ostensible purpose. In fact, since its enactment, it has been used overwhelmingly in cases having nothing at all to do with terrorism or national security. *New York* magazine revealed that from 2006 to 2009, the "sneak and peek" provision of the act (license to execute a search warrant without immediately informing the target) was used in 1,618 drug-related cases, 122 cases connected with fraud, and just 15 that involved terrorism.

But once the citizenry acquiesces to a new power, believing that it does not affect them, it becomes institutionalized and legitimized and objection becomes impossible. Indeed, the central lesson learned by Frank Church in 1975 was the extent of the danger posed by mass surveillance. In an interview on *Meet the Press*, he said:

> That capability at any time could be turned around on the American people and no American would have any privacy left, such is the capability to monitor everything—telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyrant . . . the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance . . . is within the reach of the government to know. Such is the capacity of this technology.

Writing in the *New York Times* in 2005, James Bamford observed that the threat from state surveillance is far more dire today than it was in the 1970s: "With people expressing their innermost thoughts in e-mail messages, exposing their medical and financial records to the Internet, and chatting constantly on cellphones, the agency virtually has the ability to get inside a person's mind."

Church's concern, that any surveillance ability "could be turned around on the American people," is precisely what the NSA has done post-9/11. Despite operating under the Foreign Intelligence Surveillance Act, and despite the prohibition on domestic spying embedded in the agency's mission from the start, many of its surveillance activities are now focused on US citizens on US soil.

Even absent abuse, and even if one is not personally targeted, a surveillance state that collects it all harms society and political freedom in general. Progress both in the United States and other nations was only ever achieved through the ability to challenge power and orthodoxies and to pioneer new ways of thinking and living. Everyone, even those who do not engage in dissenting advocacy or political activism, suffers when that freedom is stifled by the fear of being watched. Hendrik

Hertzberg, who downplayed concerns about the NSA programs, nonetheless acknowledged that "harm has been done. The harm is civic. The harm is collective. The harm is to the architecture of trust and accountability that supports an open society and a democratic polity."

Surveillance cheerleaders essentially offer only one argument in defense of mass surveillance: it is only carried out to stop terrorism and keep people safe. Indeed, invoking an external threat is a historical tactic of choice to keep the population submissive to government powers. The US government has heralded the danger of terrorism for more than a decade to justify a host of radical acts, from renditions and torture to assassinations and the invasion of Iraq. Ever since the 9/11 attack, US officials reflexively produce the word "terrorism." It is far more of a slogan and tactic than an actual argument or persuasive justification for action. And in the case of surveillance, overwhelming evidence shows how dubious a justification it is.

To begin with, much of the data collection conducted by the NSA has manifestly nothing to do with terrorism or national security. Intercepting the communications of the Brazilian oil giant Petrobras or spying on negotiation sessions at an economic summit or targeting the democratically elected leaders of allied states or collecting all Americans' communications records has no relationship to terrorism. Given the actual surveillance the NSA does, stopping terror is clearly a pretext.

Moreover, the argument that mass surveillance has prevented terror plots—a claim made by President Obama and a range of national security figures—has been proved false. As the *Washington Post* noted in December 2013, in an article headlined "Officials' Defenses of NSA Phone Program May Be Unraveling," a federal judge declared the phone metadata collection program "almost certainly" unconstitutional, in the process saying that the Justice Department failed to "cite a single case in which analysis of the NSA's bulk metadata collection actually stopped an imminent terrorist attack."

That same month, Obama's hand-picked advisory panel (composed of, among others, a former CIA deputy director and a former White

House aide, and convened to study the NSA program through access to classified information) concluded that the metadata program "was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional [court] orders."

Quoting the *Post* again: "In congressional testimony, [Keith] Alexander has credited the program with helping to detect dozens of plots both in the United States and overseas" but the advisory panel's report "cut deeply into the credibility of those claims."

Additionally, as Democratic senators Ron Wyden, Mark Udall, and Martin Heinrich—all members of the Intelligence Committee—baldly stated in the *New York Times*, the mass collection of telephone records has not enhanced Americans' protection from the threat of terrorism.

> The usefulness of the bulk collection program has been greatly exaggerated. We have yet to see any proof that it provides real, unique value in protecting national security. In spite of our repeated requests, the N.S.A. has not provided evidence of any instance when the agency used this program to review phone records that could not have been obtained using a regular court order or emergency authorization.

A study by the centrist New America Foundation testing the veracity of official justifications for the bulk metadata collection concurred that the program "has had no discernible impact on preventing acts of terrorism." Instead, as the *Washington Post* noted, in most cases where plots were disrupted the study found that "traditional law enforcement and investigative methods provided the tip or evidence to initiate the case."

The record is indeed quite poor. The collect-it-all system did nothing to detect, let alone disrupt, the 2012 Boston Marathon bombing. It did not detect the attempted Christmas-day bombing of a jetliner over Detroit, or the plan to blow up Times Square, or the plot to attack the New York City subway system—all of which were stopped by alert bystanders or traditional police powers. It certainly did nothing to stop the string of mass shootings from Aurora to Newtown. Major international attacks from London to Mumbai to Madrid proceeded without detection, despite involving at least dozens of operatives.

And despite exploitative claims from the NSA, bulk surveillance would not have given the intelligence services better tools to prevent the attack on 9/11. Keith Alexander, speaking to a House intelligence committee, said, "I would much rather be here today debating" the program "than trying to explain how we failed to prevent another 9/11." (The same argument, verbatim, appeared in talking points the NSA gave its employees to use to fend off questions.)

The implication is rank fearmongering and deceitful in the extreme. As CNN security analyst Peter Bergen has shown, the CIA had multiple reports about an al-Qaeda plot and "quite a bit of information about two of the hijackers and their presence in the United States," which "the agency didn't share with other government agencies until it was too late to do anything about it."

Lawrence Wright, the *New Yorker*'s al-Qaeda expert, also debunked the NSA's proposition that metadata collection could have stopped 9/11, explaining that the CIA "withheld crucial intelligence from the FBI, which has the ultimate authority to investigate terrorism in the U.S. and attacks on Americans abroad." The FBI could have stopped 9/11, he argued.

> It had a warrant to establish surveillance of everyone connected to Al Qaeda in America. It could follow them, tap their phones, clone their computers, read their e-mails, and subpoena their medical, bank, and credit-card records. It had the right to demand records from telephone companies of any calls they had made. There was no need for a metadata-collection program. What was needed was cooperation with other federal agencies, but for reasons both petty and obscure those agencies chose to hide vital clues from the investigators most likely to avert the attacks.

The government was in possession of the necessary intelligence but had failed to understand or act on it. The solution that it then embarked on—to collect everything, en masse—has done nothing to fix that failure.

Over and over, from multiple corners, the invocation of the terrorism threat to justify surveillance was exposed as a sham.

In fact, mass surveillance has had quite the opposite effect: it makes

detecting and stopping terror more difficult. Democratic Congressman Rush Holt, a physicist and one of the few scientists in Congress, has made the point that collecting everything about everyone's communications only obscures actual plots being discussed by actual terrorists. Directed rather than indiscriminate surveillance would yield more specific and useful information. The current approach swamps the intelligence agencies with so much data that they cannot possibly sort through it effectively.

Beyond providing too much information, NSA surveillance schemes end up increasing the country's vulnerability: the agency's efforts to override the encryption methods protecting common Internet transactions—such as banking, medical records, and commerce—have left these systems open to infiltration by hackers and other hostile entities.

Security expert Bruce Schneier, writing in the *Atlantic* in January 2014, pointed out:

> Not only is ubiquitous surveillance ineffective, it is extraordinarily costly. . . . It breaks our technical systems, as the very protocols of the Internet become untrusted. . . . It's not just domestic abuse we have to worry about; it's the rest of the world, too. The more we choose to eavesdrop on the Internet and other communications technologies, the less we are secure from eavesdropping by others. Our choice isn't between a digital world where the NSA can eavesdrop and one where the NSA is prevented from eavesdropping; it's between a digital world that is vulnerable to all attackers, and one that is secure for all users.

What is perhaps most remarkable about the bottomless exploitation of the threat of terrorism is that it is so plainly exaggerated. The risk of any American dying in a terrorist attack is infinitesimal, considerably less than the chance of being struck by lightning. John Mueller, an Ohio State University professor who has written extensively about the balance between threat and expenditures in fighting terrorism, explained in 2011: "The number of people worldwide who are killed by Muslim-type terrorists, Al Qaeda wannabes, is maybe a few hundred outside of war zones. It's basically the same number of people who die drowning in the bathtub each year."

More American citizens have "undoubtedly" died "overseas from traffic accidents or intestinal illnesses," the news agency McClatchy reported, "than from terrorism."

The idea that we should dismantle the core protections of our political system to erect a ubiquitous surveillance state for the sake of this risk is the height of irrationality. Yet exaggeration of the threat is repeated over and over. Shortly before the 2012 Olympics in London, controversy erupted over a supposed lack of security. The company contracted to provide security had failed to appoint the number of guards required by its contract, and shrill voices from around the globe insisted that the games were therefore vulnerable to a terrorist attack.

After the trouble-free Olympics, Stephen Walt noted in *Foreign Policy* that the outcry was driven, as usual, by severe exaggeration of the threat. He cited an essay by John Mueller and Mark G. Stewart in *International Security* for which the authors had analyzed fifty cases of purported "Islamic terrorist plots" against the United States, only to conclude that "virtually all of the perpetrators were 'incompetent, ineffective, unintelligent, idiotic, ignorant, unorganized, misguided, muddled, amateurish, dopey, unrealistic, moronic, irrational, and foolish.'" Mueller and Stewart quoted from Glenn Carle, former deputy national intelligence officer for transnational threats, who said, "We must see jihadists for the small, lethal, disjointed and miserable opponents that they are," and they noted that al-Qaeda's "capabilities are far inferior to its desires."

The problem, though, is that there are far too many power factions with a vested interest in the fear of terrorism: the government, seeking justification for its actions; the surveillance and weapons industries, drowning in public funding; and the permanent power factions in Washington, committed to setting their priorities without real challenge. Stephen Walt made this point:

> Mueller and Stewart estimate that expenditures on domestic homeland security (i.e., not counting the wars in Iraq or Afghanistan) have increased by more than $1 trillion since 9/11, even though the annual risk of dying in a domestic terrorist attack is about 1 in 3.5 million. Using conservative assumptions and conventional risk-assessment methodol-

ogy, they estimate that for these expenditures to be cost-effective "they would have had to deter, prevent, foil or protect against 333 very large attacks that would otherwise have been successful every year." Finally, they worry that this exaggerated sense of danger has now been "internalized": even when politicians and "terrorism experts" aren't hyping the danger, the public still sees the threat as large and imminent.

As the fear of terrorism has been manipulated, the proven dangers of allowing the state to operate a massive secret surveillance system have been seriously understated.

Even if the threat of terrorism were at the level claimed by the government, that would still not justify the NSA's surveillance programs. Values other than physical safety are at least as if not more important. This recognition was embedded in US political culture from the nation's inception, and is no less crucial for other countries.

Nations and individuals constantly make choices that place the values of privacy and, implicitly, freedom above other objectives, such as physical safety. Indeed, the very purpose of the Fourth Amendment in the US Constitution is to prohibit certain police actions, even though they might reduce crime. If the police were able to barge into any home without a warrant, murderers, rapists, and kidnappers might be more easily apprehended. If the state were permitted to place monitors in our homes, crime would probably fall significantly (this is certainly true of house burglaries, yet most people would recoil in revulsion at the prospect). If the FBI were permitted to listen to our conversations and seize our communications, a wide array of crime could conceivably be prevented and solved.

But the Constitution was written to prevent such suspicionless invasions by the state. By drawing the line at such actions, we knowingly allow for the probability of greater criminality. Yet we draw that line anyway, exposing ourselves to a higher degree of danger, because pursuing absolute physical safety has never been our single overarching societal priority.

Above even our physical well-being, a central value is keeping the state out of the private realm—our "persons, houses, papers, and effects," as the Fourth Amendment puts it. We do so precisely because that realm

is the crucible of so many of the attributes typically associated with the quality of life—creativity, exploration, intimacy.

Forgoing privacy in a quest for absolute safety is as harmful to a healthy psyche and life of an individual as it is to a healthy political culture. For the individual, safety first means a life of paralysis and fear, never entering a car or airplane, never engaging in an activity that entails risk, never weighing quality of life over quantity, and paying any price to avoid danger.

Fearmongering is a favored tactic by authorities precisely because fear so persuasively rationalizes an expansion of power and curtailment of rights. Since the beginning of the War on Terror, Americans have frequently been told that they must relinquish their core political rights if they are to have any hope of avoiding catastrophe. From Senate Intelligence chair Pat Roberts, for example: "I am a strong supporter of the First Amendment, the Fourth Amendment and civil liberties. But you have no civil liberties if you are dead." And GOP senator John Cornyn, who ran for reelection in Texas with a video of himself as a tough guy in a cowboy hat, issued a cowardly paean to the benefit of giving up rights: "None of your civil liberties matter much after you're dead."

Talk radio host Rush Limbaugh piled on, displaying historical ignorance by asking his large audience: "When is the last time you heard a president declare war on the basis that we gotta go protect our civil liberties? I can't think of one. . . . Our civil liberties are worthless if we are dead! If you are dead and pushing up daisies, if you're sucking dirt inside a casket, do you know what your civil liberties are worth? Zilch, zero, nada."

A population, a country that venerates physical safety above all other values will ultimately give up its liberty and sanction any power seized by authority in exchange for the promise, no matter how illusory, of total security. However, absolute safety is itself chimeric, pursued but never obtained. The pursuit degrades those who engage in it as well as any nation that comes to be defined by it.

The danger posed by the state operating a massive secret surveillance system is far more ominous now than at any point in history. While the government, via surveillance, knows more and more about what its citi-

zens are doing, its citizens know less and less about what their government is doing, shielded as it is by a wall of secrecy.

It is hard to overstate how radically this situation reverses the defining dynamic of a healthy society or how fundamentally it shifts the balance of power toward the state. Bentham's Panopticon, designed to vest unchallengeable power in the hands of authorities, was based on exactly this reversal: "The essence of it," he wrote, rests in "the centrality of the inspector's situation" combined with the "most effectual contrivances for seeing without being seen."

In a healthy democracy, the opposite is true. Democracy requires accountability and consent of the governed, which is only possible if citizens know what is being done in their name. The presumption is that, with rare exception, they will know everything their political officials are doing, which is why they are called public servants, working in the public sector, in public service, for public agencies. Conversely, the presumption is that the government, with rare exception, will not know anything that law-abiding citizens are doing. That is why we are called private individuals, functioning in our private capacity. Transparency is for those who carry out public duties and exercise public power. Privacy is for everyone else.