

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//SI//NF//NOFORN

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 “Legitimation of violence,” “Constructing experience in mind of targets which should be accepted so they don’t realize,” and “Optimising deception channels.”

These types of 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 to “cognitively infiltrate” 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.

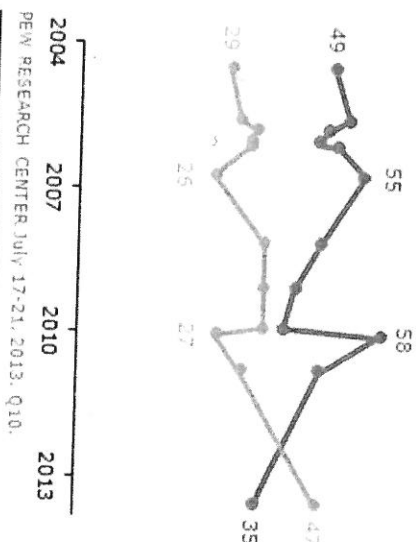
Ample polling data reflected this shift. At the end of July 2013, the Pew Research Center released a poll showing that the majority of Americans disbelieved the defenses offered for the NSA’s actions. In particular, “a majority of Americans—56%—say that federal courts fail to provide adequate limits 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.

Gov't Anti-Terror Policies Have ...

— Not gone far enough to protect the country
— Gone too far in restricting civil liberties



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 *Face the Nation* 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 Senate panel, 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 2012: "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 methodology,

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.