1

INTRODUCTION: MAKING A DIFFERENCE

AROUND THE TIME EDWARD SNOWDEN BEGAN WORKING FOR THE CENTRAL INTELligence Agency in 2006, I decided to leave my position as a lawyer for the American Civil Liberties Union in the hope I could make a difference by going inside America's growing surveillance state.[1] Surprisingly, senior intelligence officials took a chance on hiring me in a unique new office safeguarding civil liberties and privacy. My job was to advise the director of national intelligence, who oversees the seventeen agencies of the U.S. intelligence community.

Before I joined the government, I had testified before Congress as an ACLU lawyer, arguing against expanded surveillance in the "war on terror." Since information on national security surveillance was secret, my arguments were based on hypothetical scenarios about how intelligence agencies might use their new powers.[2] After joining the government I learned the truth—about bulk collection of data, the weakening of internet security, and other intrusive surveillance activities. The imaginative ways intelligence agencies were using their

legal authorities exceeded the most alarming visions I had conjured up in my years as a privacy and civil liberties activist. The government was collecting immense volumes of data both inside and outside the United States, including data pertaining to Americans, creating serious privacy risks.

For the next seven years, I worked with a growing team of internal privacy watchdogs inside the intelligence community. We reviewed the U.S. government's most secret surveillance programs. Our job was to ensure these programs had a firm basis in law and included safeguards to protect privacy and civil liberties. As surprised as I had been by the breadth of surveillance, I was just as surprised by how seriously everyone inside the government took the rules that governed it. We brought the legally questionable surveillance policies of the Bush administration under the supervision of Congress and the judiciary, and devised new oversight mechanisms to ensure compliance with the rules. Our efforts put the U.S. government's mass surveillance programs on a stronger legal basis, helping the intelligence community weather the storm when these programs became public in 2013.

While I am proud of the work I did to keep intelligence agencies in bounds, it is fair to say my success in protecting privacy as an insider was limited. In retrospect, my focus on ensuring that the intelligence agencies were true to the complex and sometimes arbitrary legal rules that govern surveillance caused me to miss the broader impact of the U.S. government's programs on the privacy of all the world's data, and what this meant for the privacy of Americans. The rules that guided my work were designed to prevent "spying on Americans." They were mostly written in the 1970s. They depended on geography and borders in a way that the internet and globalization had made largely obsolete. The digital data, communications, and personal lives of Americans now transcended national boundaries. Compounding the problem, the rules were based on analog technology. They made distinctions that no longer made much sense between types of data, offering inadequate protection in an age of digital surveillance. Inside the intelligence community, these problems were well understood, and many shared my concerns. Our efforts to start a meaningful public dialogue about privacy were largely frustrated by the decisions of top officials to keep modern programs of mass surveillance a secret.

In 2009 I was detailed to the White House national security staff to serve a stint as its first-ever director of privacy and civil liberties. Barack Obama had won election as president with a promise to review the surveillance programs initiated by President George W. Bush after the events of September 11, 2001. I had high hopes that Obama's fresh approach would force needed reforms that would protect privacy. But after Obama took office, he continued and even expanded mass surveillance programs. Despite my lofty White House perch, my broader hopes for reform proved elusive. Obama's top aides showed little interest in reforming mass surveillance until after I left, when Edward Snowden forced them to confront the issue.

In 2013 I left government to pursue research and teaching. As my work to provide privacy and civil liberties safeguards for mass surveillance programs had been highly classified, I expected I would never speak or write publicly about it. Instead, much to my surprise, I found myself thrust into a global conversation about privacy and mass surveillance. Only a few days after my formal resignation in June, the first stories based on secret documents leaked by Snowden appeared in the press. They described surveillance programs on which I had worked. That summer the Obama administration confirmed these programs and declassified details about the rules that governed them, including some of the safeguards I had helped devise.

The Snowden revelations concerned the operations of the largest of the secret "three-letter" intelligence agencies, the National Security Agency. The NSA collects "signals intelligence," which means it scoops up the world's communications, processes them into intelligible form, and turns them into intelligence reports. NSA operations are essential to national security and to international stability, but it is a challenge to reconcile them with the values of a free society. The Snowden revelations forced the NSA to take painful steps to open up. Before Snowden, basic information such as the number of targets affected by court-ordered surveillance was a closely guarded secret, obscuring important facts such as how much surveillance could be authorized by a single court order. Today the head of the intelligence community publishes an annual transparency report, revealing that one such order authorized surveillance of more than 100,000 foreign targets, and that data about Americans collected under that order were queried more than 30,000 times, among other details.[3]

This new transparency would not have happened without Snowden. "Where you're in positions of privileged access," Snowden said, "you see things that may be disturbing." During this interview from a hotel in Hong Kong, Snowden revealed himself to the world as the source of ongoing leaks of classified information. "This is something that's not our place to decide," Snowden said, explaining his decision. "The public needs to decide if these programs and policies are right or wrong."[4] Without a basic level of transparency about mass surveillance programs, the NSA's operations lack democratic legitimacy. The most secret of the government's secret agencies will never be a model of transparency. Still, it has never been more transparent than it is today.

Thanks to Snowden, the government has also been forced to become more accountable for mass surveillance. Before Snowden, the NSA used a secret interpretation of the Patriot Act, the antiterrorism law passed in 2001, to amass a nationwide database of telephone records from American companies of calls to, from, and within the United States. In 2015 a federal appeals court declared this program of bulk collection unlawful.[5] Less than a month later Congress passed the Freedom Act, which replaced this program with an alternative one that leaves the data with the telephone companies.[6] Before passage of the Freedom Act, the secret court that authorizes intelligence surveillance almost never heard more than the government's side of the argument. Now, outside lawyers routinely appear to argue the case for privacy.[7]

More fundamentally, the Snowden revelations have enlarged the way the U.S. government thinks about privacy. Before Snowden, there was no written order, directive, or policy that gave any consideration to the privacy of foreign citizens who live outside the borders of the United States. When intelligence officials asked lawyers like me about privacy, it went without saying that we were talking about American citizens and residents. In 2014 President Obama signed a directive reforming signals intelligence collection, requiring that some privacy protections apply to the personal information that agencies collect about foreigners outside the United States. By 2015 all agencies had issued new procedures, or revised existing procedures, to fulfill this requirement.[8] Today, for the first time in history, it is the policy of the United States that the privacy and civil liberties of everyone in the world must be taken into account when agencies collect signals intelligence.

The Snowden revelations have also helped the public better understand how the NSA's programs targeting foreigners affect the privacy of Americans. At the end of the Bush administration, Congress gave the government broad power to compel American companies to assist in surveillance of foreign targets with a secret court order. Section 702 of the Foreign Intelligence Surveillance Act (FISA) allows collection of data inside the United States belonging to foreign citizens outside the United States. While the law itself was no secret, Snowden leaked the existence of two programs authorized by section 702, the Prism program and "upstream collection." Prism, also known as "downstream collection," allows the NSA to obtain stored e-mails and other communications from American technology companies. Upstream collection gives the NSA access to data in transit across the internet backbone facilities of American telecommunications companies.[9] Both programs permit what critics call a backdoor search: routine queries by other agencies about Americans who may be in contact with the NSA's foreign targets or who may be mentioned in e-mails or other communications. This practice has now been limited, although critics would like stricter limits, including warrants.[10] Such privacy issues used to be known only to people like me: those privileged to attend classified briefings or to participate in the secret proceedings of the Foreign Intelligence Surveillance Court.

In short, the Snowden revelations have made the NSA more transparent, more accountable, and more protective of privacy. Surprisingly, the reforms have also made the NSA more effective. Jack Goldsmith, a former Justice Department official in the George W. Bush administration, marveled in June 2016 that "the intelligence community, and especially the NSA, have emerged in astonishingly good shape" in the aftermath of the Snowden revelations.[11] For example, the system Congress created to end the NSA's bulk collection of telephone records from American companies actually gave NSA analysts access to a broader volume of data than before. This allowed the agency to collect more than 151 million records in 2016, without the NSA having the responsibility for storing the billions of records it used to collect each day under the old program.[12]

Former attorney general Eric Holder has offered warm words for Snowden. "We can certainly argue about the way in which Snowden did what he did, but I think that he actually performed a public service

by raising the debate that we engaged in and by the changes that we made," he said in May 2016.[13] Holder's praise raised eyebrows. After all, he was the attorney general when Snowden was charged with serious felonies, including theft of government property and disclosure of classified communications intelligence. I found Holder's views less surprising than many did. I had heard similar views expressed privately by several of my colleagues in the national security community.

WHEN I JOINED THE INTELLIGENCE community, I wondered if I would be able to make a difference. My hope was that my position of privileged access would allow me to argue for privacy in a way I never could have done as an outside advocate. The post-Snowden reforms described in this book are more significant than any my colleagues and I achieved during my time in public service. That it took a Snowden to force these changes made me question whether I had done the right thing by working within the system. While I kept my promise not to spill the government's secrets, Snowden's strategy proved more effective than mine. Snowden explained his decision to leak classified information as an act of self-sacrifice, motivated by patriotism. Many do not believe Snowden's claims about why he did what he did, regarding him as an attention-seeking opportunist. Some even speculate (without much evidence, it should be said) that he acted in concert with Russian or other foreign intelligence services.[14] Whatever Snowden's true motives, it is undeniable that he made a difference. Snowden has said that his greatest fear when he decided to give his purloined documents to journalists was not that he would be imprisoned but that no one would care, and "nothing will change."[15] That fear has not been realized. The post-Snowden reforms represent the first real step toward addressing the privacy issues posed by mass surveillance.

Of course, Snowden's strategy also resulted in substantial costs—to Snowden himself and to American national security. Snowden not only told the world about the NSA's impact on global privacy, he also compromised many legitimate programs focused on China and other potential adversaries of the United States, and in some cases compromising these programs lacked any obvious privacy or civil liberties benefits, even for foreign citizens.[16] Many of these revela-

tions caused the NSA relatively little embarrassment but did result in damage to national security. They received little attention, at least in the American press, but were carefully noted by foreign governments. For reasons involving national security—but also because of excessive secrecy and bureaucratic inertia—it has been difficult for officials to make this case in public in a compelling way, but that does not make the damage from Snowden's disclosures less real.

Was the damage worth it? Geoffrey Stone, a law professor at the University of Chicago and a former colleague of President Obama, served on a review group Obama appointed in 2013 to scrutinize NSA programs and recommend reforms. "To say I was skeptical about the NSA is, in truth, an understatement," he told the NSA in a speech to its employees after the review was complete. To his surprise he found, as I had, that the NSA "operates with a high degree of integrity and a deep commitment to the rule of law." The NSA was doing what it had been told to do: the agency's employees were being "demonized" unfairly for decisions made "not by them, but by Presidents, the Congress, and the courts."[17] These decisions, Stone and his colleagues found, had resulted in unacceptable privacy risks, requiring significant reforms.

The fact that a series of massively damaging leaks was needed to achieve such sensible reforms can only be described as a failure of leadership. For me, that failure is at least in part a personal one. As a privacy and civil liberties official inside the intelligence community and later at the White House, I was supposed to provide top officials with confidential advice about how to ensure that intelligence programs protected our liberties. In essence, I was to be an authorized whistleblower for classified programs—a sort of official Snowden. In performing that role, I tried to make just the kind of arguments about privacy and NSA surveillance that many have said Snowden should have raised internally instead of compromising classified information. Unlike Snowden, I had direct access to the officials who could have made surveillance reform a reality—and who did so, after the Snowden leaks forced their hand. I can say from experience that there is simply no way that Snowden, a junior NSA contractor, could have accomplished more to reform mass surveillance by working inside the system.

"MASS SURVEILLANCE" IS A TERM that rankles my old colleagues in the intelligence community, and for good reason. Many object to its imprecision, arguing that it lumps together programs in which the NSA collects all the data traveling across a communications channel, a form of surveillance known as bulk collection, with more targeted forms of signals intelligence that nevertheless involve surveillance of many, many targets without prior, individual judicial review. These distinctions matter both in the law and in the privacy implications of particular signals intelligence programs. The indiscriminate use of a term like mass surveillance may elide these distinctions and confuse the debate, as has happened at times in discussions between American and European officials about privacy.

A more fundamental objection is that describing the NSA's programs as mass surveillance is simply unfair. The NSA is not interested in ordinary people but in finding terrorists and other valid intelligence targets, and it collects masses of information only in order to find those targets. The term *mass surveillance* conjures up visions of totalitarianism. Intelligence officials prefer to describe the NSA's vast surveillance operations as *signals intelligence*, a term associated with battles against totalitarianism, evoking American and British successes in reading enemy communications in World War II and later conflicts.

Perhaps the most effective organization to engage in mass surveillance for social control in history was the Ministry for State Security of the German Democratic Republic—the feared Stasi of East Germany. With German thoroughness, the Stasi ran a far more pervasive surveillance apparatus in defense of a Communist dictatorship than the Soviet Union did. The Stasi amassed 6 million files during its history, a figure amounting to more than one-third of the East German population. At its height, it employed one secret policeman for every 166 East German citizens, a ratio that shrinks to one informer for every 6.5 citizens when part-time agents are included. About 2,000 Stasi officers were used to tap 100,000 telephone lines in West Germany and West Berlin.[18]

These numbers seemed alarming when East Germany collapsed and the secrets of the Stasi were revealed. They seem almost quaint in the age of Snowden. The NSA collects far more data about ordinary

people than the Stasi ever did, using far more sophisticated technology. Given the amount of digital data that the NSA obtains on a daily basis without anything like a search warrant, I believe that to describe what the NSA does as mass surveillance is simply a statement of fact, and that to insist on euphemisms like "collection of signals intelligence" is to deny this inconvenient truth. Nevertheless, the debate over the NSA's mass surveillance programs merely begins and does not end with this acknowledgment. While the idea of mass surveillance vividly captures the risks involved in what the NSA does, the NSA is nothing like the Stasi, an agency that amassed private information on perceived enemies of a totalitarian state as a weapon to defend a closed society.[19] The NSA serves the most diverse, complex, and free society the world has ever known, operating under a variety of imperfect, outdated, and often inadequate rules, struggling to do its best to provide intelligence to its democratically elected officials and to keep people safe not only in the United States but around the world.

In his polemical account of his role in the Snowden affair, Glenn Greenwald argues that the NSA's true objective is not to provide intelligence that can stop international terrorism and achieve other worthy objectives but to induce social control by destroying privacy. "The US government had built a system that has as its goal the complete elimination of electronic privacy worldwide," he claims.[20] If Greenwald is right, the answer is easy. End mass surveillance—which is to say, most of what the NSA does. Those of us who believe that the NSA's far-flung operations are essential to national security and global stability have the harder task of keeping the agency's mass surveillance capabilities under control.

Keeping intelligence agencies under control has rarely been more urgent. Presidents have abused surveillance powers in the past. During the 2016 presidential campaign, Donald Trump gave a vague but alarming answer to a reporter's question: "Do we need warrantless searches of Muslims?" In an answer that almost went unnoticed, Trump replied in the affirmative, saying, "We're going to have to do things that we never did before," dismissively noting that "some people are going to be upset about it."[21] President Trump's unusually fraught relationship with his own intelligence community could also result in abusive surveillance in an effort to ferret out leakers or other perceived enemies within. While the United States has a robust system

of intelligence oversight—arguably the strongest in the world—it still largely depends on the good faith of intelligence officials and those who oversee them. It is a delusion to believe that the NSA or other intelligence agencies are now tyrant-proof. In Snowden's first interview, he warned against "turnkey tyranny." He worried the NSA was building an "architecture of oppression" with its mass surveillance programs. One day, he said, "a new leader will be elected" and "they'll flip the switch."[22] It is important that this warning not be proved prophetic. Despite the surveillance reforms of the past four years, it is not nearly hard enough for a would-be tyrant to turn the key.

It is time to move beyond Snowden. He deserves our thanks for this round of surveillance reform, but while his strategy is effective, it is not sustainable. The public should not have to rely on employees of the NSA and other agencies to leak information about the government's most sensitive programs in order to forestall abuse. One way to judge success in the struggle to reform the NSA and other intelligence agencies is to ask what a friend might tell a future Edward Snowden, if he were to ask that friend whether he should reveal the government's deepest surveillance secrets in order to launch a new conversation on privacy, at great personal cost and despite serious risks to national security. If surveillance reform is a success, the friend could tell him with confidence that such a course of action was simply not necessary. Surveillance agencies are following the rules at least most of the time. They are adapting when those rules become obsolete. Checks and balances are working.

We are not there yet—not by a long shot. There is much more to do.