Introduction

Technology can be a force for good – connecting people, enabling creativity, making knowledge widely available, and empowering communities to work together. But the Internet and other digital technologies have also profoundly transformed government capabilities to spy on people, in ways that raise important questions about how to protect civil rights and political freedoms. This book explains the law and policy of American digital surveillance in the modern era. It invites the general public to participate intellectually and politically in securing a future where technology promotes free and open exchanges, while also protecting citizens in their daily lives, and providing for law enforcement and national security.

When I first began researching the relationship between surveillance, technology, and civil liberties, the digital era was in its infancy. I became a lawyer in the 1990s in the early years of the public Internet. I represented people charged with crimes related to the Internet in state and federal courts. I also litigated Fourth Amendment privacy claims, seeking constitutional protection for the wealth of personal data that new technologies were just beginning to generate. My clients included computer security experts, who were being investigated for technology research that scared judges unfamiliar with the Internet, as well as run-of-the-mill criminal defendants facing digital evidence like door access logs, hard drive searches, and more. I learned how hard it was to educate judges about technology. Once, when questioning the forensic reliability of a document purporting to log user access to an important computer server, I argued that the entries were not authenticated, but cut and pasted into a Microsoft Word document and thus could be incomplete or manipulated by a police officer or prosecutor. "Cut and paste?" the judge asked. "Like, with a scissor?"

I came to Stanford in 2001 to teach, research, and advocate for better technology-related policies. One of the major mysteries scholars and civil libertarians were confronting was surveillance policy. A major obstacle to understanding government surveillance is the veil of secrecy that

surrounds our national security policies. I am concerned with the toll surveillance can take on personal freedom. How can we know whether surveillance conducted in secret is constructive or destructive? For years, surveillance and civil liberties lawyers like me have been wondering what the US government is really doing when it spies on regular people. We've submitted Freedom of Information Act (FOIA) requests for records about surveillance technologies. We've filed lawsuits challenging certain surveillance statutes as indiscriminate. We've interviewed whistleblowers, who have revealed how US spying impacts the privacy and freedom of people around the world. Still, the big picture was hazy. Each time surveillance news broke, lawmakers and the public cared more about other things and the story faded off the front pages. As with our government's top-secret classification of other "war on terror" policies – drone strikes, waterboarding and other torture techniques, kidnapping people and bringing them to off-the-books black sites for imprisonment, interrogation, or worse – we suspected that the secrecy was hiding ill-advised, illegal, and even dangerous activity.

Then came June 2013 and Edward Snowden. Snowden, a former contractor for the secretive National Security Agency (NSA), gave reporters documents, evidence that can't be ignored, and demonstrated clearly that American spying is out of control. The United States is collecting vast amounts of private data, including about American citizens and even more about people around the world. Behind closed doors, judges are making secret law, adopting laughably bad interpretations of statutes, and invalidating constitutional privacy protections in the name of spying on innocent people. Spies are hacking the Internet, installing malicious software, and stealing encryption keys so that they can carry on mass surveillance. Computers are collecting sensitive, detailed data, reading emails and recording the phone calls of millions of people. Social welfare organizations, groups we think of as doing good – UNICEF, Doctors Without Borders, the Council on American Islamic Relations (CAIR) – are surveillance targets. Snowden's disclosures also revealed that the NSA had proposed using the information it serendipitously collects on pornography viewing and personal foibles to discredit people the agency says hold radical, albeit peaceful, political beliefs. We're reminded of the Federal Bureau of Investigation's (FBI) dirty tricks campaigns against the civil rights and antiwar movements of the 1960s and 1970s. Now, as then, agents use data gleaned from potentially illegal spying in criminal courts and mislead defendants and even judges about where it comes from.

As University of Pennsylvania computer science professor and cryptographer, Matt Blaze, said to me soon after the Snowden stories started to break: "Isn't finally knowing all this great? … Except for how terrible it all is."

Yes, it is great. It's great to finally have some answers. After years of being told that civil libertarians were needlessly alarmist about surveillance, policy makers are finally acknowledging the validity of our concerns. We are learning what kind of spying the US government has been doing in our name. It's great, as a surveillance lawyer, to finally get behind the veil of secrecy to learn what courts think our privacy laws actually mean. It's great to have an opportunity to debate openly as a democracy how to protect our privacy and security, how to promote civil liberties and human rights around the world.

But as Matt's quip pointed out, the Snowden revelations also confirmed civil libertarians' worst fears. Modern surveillance is truly different and far more dangerous than we had previously understood. Modern surveillance uses more powerful spying technology, operates under weaker privacy laws, is motivated by a far greater hunger for data following the terrorist attacks of September 11th, and is shrouded in secrecy. For these reasons, the truth about modern surveillance is different from what the public might understand in important ways.

First, modern surveillance is mass surveillance. It used to be that governments did not collect much information on regular people. Governments were technologically limited in their capacity to spy. Now, the NSA can collect vast amounts of information, and then parse through it for matters of interest. Increasingly, protections against abuse, if there are any, operate after-the-fact. That means the US government used to lack the *capacity* for widespread abuse of information because it had limited ability to collect the data. Now, the government has limited *permission* to misuse the massive amount of information it obtains through surveillance.

Next, modern surveillance targeting foreigners has a huge impact on American privacy, as our data gets caught in any dragnet installed on the global Internet. Many people do not realize that our failure to respect the privacy of foreigners impacts Americans too. This is because the image of Spy vs. Spy is now outdated. Modern surveillance means spying on regular people around the world, not just government agents, terrorists, and other spies.

Third, spying is thriving, in part because of technology. Modern surveillance is rapidly defeating constraints posed by either technology

or economics. It used to be impossible to follow thousands of people 24 hours a day while ensuring that none of them would ever find out. Today it's not only possible, it's cheap and it's easy. It's not that much more trouble to track hundreds of thousands or millions of people than it is to follow a few.

Spying is thriving not only because of technology, but also because of modern business models. Much of the modern privacy problem is the result of people giving up their data – knowingly or otherwise – to obtain cool new products and services. American spies are successfully deploying surveillance-friendly communications tools even where we could have more privacy-protecting ones. That means building secret spying rooms inside phone company offices, compromising encryption standards, forcing back doors in communications products like Skype, weakening encryption protection for iPhones and Android devices, and more. Modern surveillance is increasingly hard coded into technology and wedded with business models, making it more resistant to legal and political change and capable of abuse on an ongoing basis.

Fourth, in the face of these imperatives – technology, economics, and consumer demand – law has fallen way behind. Modern surveillance is regulated by a confusing patchwork of laws that nevertheless fails to provide meaningful limits on government power, and which therefore invites abuse. After September 11th, laws that should have protected people's privacy and stopped surveillance abuses were weakened via the USA PATRIOT Act. When technology and economics gave spies vastly more power, rather than have law step up to the challenge of constraining that power, Congress and the courts did nothing, or the laws were softened even further. American spies have flooded into the power vacuum left by powerful technology and weak legal protections. While the public knew Congress was rolling back privacy laws to some extent with the USA PATRIOT Act, those decisions actually have led to far greater privacy invasions than anyone understood before now.

Finally, modern surveillance depends on an untenable level of secrecy. Spying has always protected legitimate secrets from the targets. But now since everyone is subject to spying, modern surveillance has to be hidden from everyone. The activities of American spies remain hidden from public oversight. That means secret court opinions, classified policies, misleading use of language, aggressive prosecution of whistleblowers, spying on journalists, and suppressing court challenges. These practices are fundamentally incompatible with a free society.

The call is clear. We need a comprehensive public investigation into what American spies are doing in our name, and we need far stronger regulation of surveillance activities to protect innocent people's privacy and to guard against abuses of sensitive, personal data.

But stunned and alarmed as many people were by Snowden's revelations, it seems that some of my friends and colleagues are in denial. They are comforted by deceptive reassurances, like when President Obama intones that "no one is listening to your phone calls." Or they insist: "I'm just a regular person, why would the government be spying on me?" They say, "massive surveillance is just the price we have to pay to keep our country safe from terrorists." Or they believe that legal reforms adopted after the surveillance abuses of the 1960s and 1970s – when the US government spied on and attempted to blackmail Dr. Martin Luther King, Jr. – remain effective today, and that the courts and Congress exercise sufficient oversight of American spies.

The truth is sobering. American spies collect billions of calls, emails, and other communications data on hundreds of thousands or millions of people without any reason for suspicion. American spies compile details that reveal the identities of people you talk with, what you read, what you buy, what you believe, and where you go. In conducting all this surveillance, American spies end up spying on Americans and are increasingly omniscient.

No doubt, terrorism is terrible. It violently destroys lives, inflicts economic loss, and robs the public of peace of mind and quality of life. It exacerbates social and class divisions and tears at the fabric of national unity. The attacks of September 11 were horrific. To this day, I cannot think about them without tearing up. But the risk terrorism poses to American lives is actually tiny. In the past decade, the number of people in the United States killed by terrorists is less than 100.[1] So why have the American people sacrificed so much of our liberty, and endangered the liberties of others, in the fight against terrorism?

America can survive terrorism. But American democracy cannot survive modern surveillance. Privacy is key to the exercise of individual

[1] Counting terrorist deaths depends on definitions. In October of 2015, an expansive definition that included non-jihadist attacks tallied seventy-one. See L. Qiu. "Fact-checking a comparison of gun deaths and terrorism deaths." *PolitiFact.* October 5, 2015. www.politifact.com/truth-o-meter/statements/2015/oct/05/viral-image/fact-checking-comparison-gun-deaths-and-terrorism-/. If you add the fourteen people slain in the December San Bernardino shooting and the three killed in the Planned Parenthood attack in November of that year, the number is still less than 100.

freedoms – to read, to think, to express oneself, to conduct intimate relationships, to be let alone. But privacy is also key to political evolution. Without a zone of protection, those who seek to evolve the country's laws and policies, to challenge the status quo, are at risk of imprisonment or blackmail by those in power. Those in power are at risk of blackmail or embezzlement by other powerful people. Americans natively understand this is true in despotic countries. We worry that China is punishing religious minorities, political upstarts, and artists. We know that in Russia journalists and business leaders with political ambitions are imprisoned or worse. These kinds of civil liberties attacks have happened here in the United States, too, still happen more than they should, and could become a serious challenge to our democracy in the future. This claim may seem hyperbolic, but while the US government is not going to dissolve into despotism overnight, the encroaching loss of liberty is profound.

This book offers a historical account of an extraordinarily complex policy and legal debate on modern surveillance. There are multiple federal agencies charged with protecting the United States' national security and foreign affairs interests as part of the so-called "intelligence community." Data collection of all kinds, including electronic surveillance, signals intelligence (SIGINT), and human intelligence (HUMINT), are part of this work. The agencies' roles can be overlapping, coordinating, or exclusive, and each of the agencies has its own mission, its own jurisdiction, and its own rules. The NSA is responsible for SIGINT. The Central Intelligence Agency (CIA) is responsible for "national foreign intelligence." The Department of Defense collects both national and military foreign intelligence. The FBI conducts counterintelligence inside the United States and when requested by other intelligence community agencies, assists with the collection of foreign intelligence inside the United States. Other members of the seventeen agencies comprising the intelligence community include the Department of Treasury, the Department of State, and the Department of Energy.[2] Collectively, I call the federal agencies involved in SIGINT collection "American spies."

Against this complicated backdrop, my job is to assess and, where appropriate, debunk American spies' best arguments for the legality and

[2] See www.dni.gov/index.php: Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, and Navy Intelligence.

acceptability of their actions. I hope to answer the questions I've been hearing from colleagues, students, friends, and the general public ever since the first news story based on Snowden documents, and enable readers to participate meaningfully in the sometimes seemingly arcane policy debates around modern surveillance.

My first goal in writing this book is to give the American voter the information she needs to understand and participate in this debate, and to make a difference. Second, I believe that by explaining the policy debates taking place in the United States, people in other nations will be able to learn from our experience, and avoid making the same mistakes that we have made.

The rules by which the government decides whether and when to respect our privacy and leave us alone, or collect information on us and eavesdrop in our private affairs, are byzantine. Today, a smattering of sparse, mostly secret internal rules is the only thing standing between people and abusive exercise of that power. As Edward Snowden said, in explaining his decision to come forward, "I believe that at this point in history, the greatest danger to our freedom and way of life comes from the reasonable fear of omniscient State powers kept in check by nothing more than policy documents." In other words, massive surveillance used to be impossible. Today, it's happening, and the risks of this extensive spying are managed with internal policies. It is not enough to try to contain overbroad surveillance with government agency protocols. These protocols are complicated and secret. When people break them, it has taken the public years to find out, and no one gets punished.

But an informed electorate is a powerful electorate. Public pressure stymied the rampant political spying of the 1960s and 1970s. In 2012, public pressure stopped SOPA and PIPA, seemingly unstoppable draconian copyright laws that would have improperly censored the Internet. And in 2015, public pressure turned network neutrality, an arcane but important issue of government regulation of Internet service providers, into a concrete rule intended to preserve and promote a free and open Internet. Similarly, Congress put an end to the NSA's bulk collection of Americans' phone records with 2015's USA Freedom Act. It can be done.

And it must. John Gilmore, one of the founders of the Electronic Frontier Foundation, is quoted as having said, "*never give a government a power you would not want a despot to have*." The American government has such powers. It has huge and growing technological capability to collect and analyze vast amounts of data. The stakes are incredibly high and time for change is short. Otherwise, mass surveillance will become – technologically and politically – the new normal.

Mass surveillance and democracy are fundamentally incompatible. It is impossible to know whether judges, lawmakers, and presidents are acting out of principle and allegiance to their understanding of what the public wants or out of fear that spies will disclose embarrassing or illegal behavior. Massive surveillance thwarts citizens pressuring for political change through the risk of criminal prosecution, blackmail, or other threats. The secrecy and the lies required to spy on everyone are inconsistent with a democratic government of, by, and for the people.

I hope this book will enable people to fight for democracy.