Preface

Surveillance is a key feature of modern American life. Toll booths monitor drivers on the interstate, and social media gather information from users for marketing data. Many people are unaware that when they use websites like Google and Amazon they enter into an agreement that allows retailers to track them for commercial purposes. In the name of national security, the government gathers information on most citizens. Surveillance, particularly government surveillance, constitutes one of the great social and legal tensions of the twenty-first century. How do we embrace technology's magnificent, egalitarian promise of equal access to information for all citizens and use state-of-the-art surveillance tactics that can promote safe communities while also upholding traditional civil liberties and individual privacy?

These concerns are not only philosophical or constitutional conundrums but also practical ethical and legal matters. Cell phone tracking provides a good example of the kind of real-world problems presented by the use of surveillance. Law enforcement agencies commonly use a single cell tower to place a suspect at the scene of a crime, even though defense lawyers have challenged the practice and have shown that it is scientifically unreliable and inaccurate.

If a reporter records a conversation without informing the interviewee (a procedure that is legal in several states), most people would consider this practice unethical or underhanded, or at least a violation of trust. When the government gathers "metadata"[1] from the phone calls of millions of citizens, is this also unethical or a violation of trust?

The articles presented in this volume explore these ideas and how what is done in the name of public safety goes to the core of our country's values.

Surveillance In the Name of Public Policy

In *Olmstead v. United States* (1928), the United States Supreme Court ruled that police could issue warrantless wiretaps on phone conversations. This decision (overturned nearly 40 years later) found that the language of the Fourth Amendment protecting citizens against arbitrary search and seizure did not apply because telephone wires reached well beyond the walls of a private residence. "The intervening wires are not part of his house or office, any more than are the highways along which they are stretched," Chief Justice William H. Taft wrote in the majority opinion.

As with many important court rulings on government surveillance, the case that necessitated the ruling was related to enforcing a major public policy of the time, Prohibition. The government viewed wiretapping as necessary to stamp out bootlegging, which had emerged as a lucrative, and illegal, import and distribution industry.

In the 1960s and 1970s, to counteract civil rights, antiwar activists, and other radicals, the FBI initiated the Counter Intelligence Program (COINTELPRO), which involved massive surveillance, infiltration, and disruption of domestic political groups. Policy makers would later view many of these methods as unnecessary and unconstitutional.

After the attack on the World Trade Center and Pentagon in September 2001, the government, whose case for surveillance was never more forceful, used surveillance on a grander scale than ever before in order to counter faceless enemies and prevent possible repeated terrorist attacks.

Passed in October of 2001, the USA PATRIOT Act became the legislative prototype for preventive surveillance policy in the post-9/11 world and provided the legal tools to advance a national security policy intended to thwart immediate threats to the United States. A key element of the program expanded the federal government's ability to gather data on private citizens and to search telephone, email, and financial records without a court order. Had the act been drafted and considered during a time of peace, it most likely would not have gained much traction but rather would have generated public debate and scrutiny. Instead, in an atmosphere of fear, Congress passed and the president signed a bill with far-reaching and unforeseen consequences.

Big Data in the Private Sector

The expanded use of telephone and Internet surveillance is part of most Americans' daily lives from the moment they wake up and check their smart phones. And as policy makers make the case for increased levels of surveillance as a means toward a safer country, the government has sought to leverage major, private-sector advances in data collection to achieve its national security aims.

Following 9/11, the NSA began working with American telephone companies, which provided access to domestic calling records and company analysis of calling patterns. This was not legal at first, but executive authority made it so in the hope that the information would present a potentially potent tool in the war on terror.

Four Internet and telephone metadata and content collection programs were created under executive authority, deemed the President's Surveillance Program, or PSP. Created during a time of crisis by some of President George W. Bush's top aides, NSA chief General Michael Hayden, and Vice President Dick Cheney, PSP circumvented checks put in place by the Foreign Intelligence Surveillance Act decades before and granted the NSA broad reach into American territories and Americans living overseas. The Foreign Intelligence Surveillance Act (FISA) court wasn't notified of the program at the outset and it would be nearly six years before the PSP would be placed under FISA's jurisdiction.

Ultimately, these programs were halted in 2011 because they did not reach the level of efficacy intended–not because of the prevailing concerns related to privacy, a lack of court orders or, in many cases, the absence of probable cause.

In 2013, Edward Snowden, a government contractor working for the National Security Agency, leaked thousands of classified documents that showed the extent of global surveillance programs, revealing for the first time that the U.S. government was collecting the phone records of most of its own citizens. The documents he leaked fortified the concerns of civil libertarians and intensified the current debate around the balance between national security and information privacy. Since the leaks, two important court rulings have split on the constitutionality of the NSA's

bulk collection of telephone metadata, and one recent ruling has stated that the NSA's program, while constitutional, has reached beyond its intended scope.

In December 2013, a federal judge ruled that the government's collection of domestic phone records is unconstitutional. The judge, U.S. District Judge Richard Leon, said the National Security Agency's bulk collection of metadata violates privacy rights. The ruling pushed back at the government's argument that a 1979 Maryland case, *Smith v. Maryland*, provided precedent for the constitutionality of collecting phone metadata, noting that public use of telephones had increased dramatically in the past three decades. In that case, the U.S. Supreme Court ruled that authorities did not need a warrant to install a pen register, or an electronic device that records all numbers called from a particular telephone line, because it did not constitute a "search" as defined by the Fourth Amendment.

However, just days later in December 2013, the NSA scored a victory when a U.S. District Judge William Pauley of New York ruled NSA's bulk collection of phone records under Section 215 of the USA PATRIOT Act was, in fact, legal. Section 215 was among the programs revealed in Snowden's classified leaks.

Striking a Balance

In May 2015, a New York federal appeals court ruled that the NSA's phone record collection program is illegal, signaling a setback for congressional leaders who favored reconstituting the Section 215 statute as its June 1 expiration approached. The ruling, however, did not question the constitutionality of Section 215 or order the program to cease; however, in the years since the act's passage and with the hindsight of a protracted military campaign, there has been increasing political pressure to strike a balance between safeguarding civil liberties and assuring national security.

On June 1, 2015, Section 215 of the USA PATRIOT Act expired, and the May ruling of the New York federal appeals court helped pave the way for a new federal bill designed to rein in government surveillance, the USA Freedom Act. The Freedom Act overwhelmingly passed in the House of Representatives by a vote of 338-88 and, on June 2, after much deliberation also passed in the Senate by a vote of 67-32, despite a strong and vocal opposition led by Senator Mitch McConnell. President Obama signed the bill hours later. Among other things, this act ended the government's bulk collection and storage of phone data, but as the divisive vote in Congress indicates, the act did not end the debate.

Matthew Brian Hersh

Note

1. In this case, metadata is a form of transactional information. It does not specifically document an individual's action as does a wiretap or surveillance video, but, if collected en masse, metadata can paint an accurate picture of someone's daily activities: where she or he goes and whom she or he calls.

1
National Security Versus Personal Privacy

Photo by Erkan Avci/Anadolu Agency/Getty Images

On October 26, 2013, demonstrators march through Washington, DC, toward the National Mall for a rally to demand that U.S. Congress investigate the National Security Agency's mass surveillance programs.

The Digital Invasion: Privacy Versus Secrecy in the Digital Age

The September 11, 2001 (9/11), terrorist attacks on the United States initiated a transformative period in American culture. Given the nature of the threat, the U.S. Government made broad changes to domestic and foreign security policies, including granting increased and often-unregulated powers to security and intelligence organizations to conduct surveillance operations. From 2002 to 2015, federal and state agencies conducted mass surveillance operations that included intercepting mobile telephone calls, text messages and emails, tracking online purchases and browsing, creating databases of images for photo recognition, and conducting widespread video and aerial surveillance operations.

Controversial surveillance operations have raised questions about personal privacy. While federal and state agencies collect and analyze information as part of a broader effort to prevent terrorism, critics argue that mass surveillance violates rights to privacy under the Fourth Amendment. The debate over security versus privacy also raises the question of ownership regarding data shared through private digital networks and whether new regulations are needed to protect the privacy of information given to third-party Internet and communications companies.

History of Domestic Surveillance

Governments have always watched their citizens. In Ancient Rome, emperors created legions of spies to watch over the populace for threats of insurrection. During the "Reign of Terror" of the French Revolution, from 1793 to 1794, Robespierre and his cadre employed surveillance committees to infiltrate and observe the population, eventually targeting as many as 500,000 "suspicious" individuals who were arrested, detained, or interrogated for connections to the former nobility.

The American government began conducting domestic surveillance in the 1920s, with the controversial Black Chamber program created by cryptologist Herbert Yardley. In 1931, Yardley published a book, *The American Black Chamber*, detailing his involvement in the program, which involved collecting and monitoring telegraphs, with the compliance of companies like Western Union. Yardley's surveillance program was disbanded in 1929, with Secretary of State Henry Stimson issuing a statement that reportedly contained the now famous statement "Gentlemen do not read each others' mail."

A similar surveillance program, Operation SHAMROCK, was created during World War II, monitoring communications with the compliance of Western Union, ITT, and RCA Global. This led to the establishment of the National Security Agency (NSA) in 1952, in an effort to counter the perceived threat of Soviet

intelligence and spy networks. The "Cold War" lasted from the end of World War II (around 1947–48) to at least the early 1990s, and resulted in a vast escalation of domestic and foreign surveillance programs. In 1975, a series of Senate hearings, the "Church Committee Hearings," were organized to investigate surveillance and privacy. The committee recommended reforms and, in 1978, Congress signed the Foreign Intelligence Surveillance Act (FISA), stipulating that government agencies needed to obtain special warrants before they could spy on American citizens.

In the wake of 9/11, the George W. Bush administration signed laws that gave the NSA and CIA the ability to conduct surveillance without adhering to FISA guidelines.

According to the digital rights group Electronic Future Foundation (EFF), in early 2002 information began to surface indicating that the NSA was engaging in warrantless wiretapping of American citizens. AT&T technician Mark Klein revealed classified data that AT&T was developing a software system that allowed the NSA to capture and analyze cellular communication. The EFF filed suit against AT&T in 2007, charging the company with illegally selling customer data. As a result, Congress passed H.R. 6304 in 2008, an amendment to FISA granting companies that cooperated with the NSA immunity from prosecution.

In 2013, former NSA and CIA analyst Edward Snowden leaked confidential CIA and NSA documents to reporter Glenn Greenwald of the *Guardian* and several American journalists. In June 2013, *The Guardian* and *The Washington Post* published articles revealing details of the NSA PRISM program, which collects stored Internet data from companies like Google Inc. and Yahoo!, for analysis. Snowden was charged with theft and fled the United States.

In October 2013, it was revealed, from the leaked documents, that the NSA collected more than 250 million email views and contact lists from Facebook, Google's Gmail, and Yahoo. In 2014, an article in *The Guardian* revealed that the NSA was also collecting millions of text messages each day in an "untargeted" surveillance sweep. Further revelations in 2014 showed that the NSA was collecting information from webcams and that the NSA's MYSTIC program could record 100 percent of the phone calls coming out of a country. In May 2014, James Risen and Laura Poitras revealed that the NSA was collecting millions of facial images from web images to be used in the creation of facial recognition programs. Journalists Glenn Greenwald and Laura Poitras, who wrote some of the first articles about the Snowden leaks, became editors of the Internet publication *The Intercept,* which continued publishing documents and analysis from Snowden in 2014 and 2015.

Privacy and the Constitution

The United States Constitution does not explicitly and distinctly guarantee a person's right to privacy. However, specific provisions of the Bill of Rights can and have been used to protect personal privacy. The First Amendment, which protects free speech, expression, and the right to "assemble" has been used to protect the privacy to hold beliefs and political views. The Third Amendment, which specifically prohibits the government from forcibly taking property from private owners, has been

used to guarantee privacy inside a person's home. The amendment that directly applies to NSA surveillance is the Fourth Amendment, ratified in 1791, which guarantees freedom from "unreasonable searches and seizures."

The Fourth Amendment is the cornerstone of privacy from government intrusion, establishing the legal principle that federal and state authorities must be able to demonstrate compelling cause before searching or confiscating an individual's property, documents, or communication records. While initially applying primarily to written correspondence, digital privacy advocates have argued that Fourth Amendment provisions should apply to digital communications as well. However, the 1979 case of *Smith v. Maryland,* (and similar rulings in the 1960s and 1970s) established that sharing data with a third party, in some situations, relinquished an individual's "expectation of privacy."

As third party sharing is a legal issue regarding the privacy of information, politicians and rights advocates have been struggling to address the issue of ownership with regard to mobile and digital communication. The public telephone system is considered a public trust, and as such, telephone communications are afforded a degree of privacy. Other types of communications, including involvement in social media, email, and other digital transmissions, are not protected under the same provisions. In general, the company providing transmission of the data in question establishes ownership of digital data through corporate policy. A review of Facebook policies, for instance, indicates that any data posted on a person's Facebook site becomes the property, in part, of Facebook. This is the provision that allows Facebook to donate or sell a person's private data to other companies or to government agencies.

In the 2010 case of *U.S. v. Warshak,* the Sixth Circuit Court of Appeals ruled that the government needs a court order to seize email communications, thus effectively extending protections afforded to telephone and U.S. mail to email communications as well. The 2010 case was one of several modern challenges to government surveillance and attempts to establish rules regarding the privacy of digital communications. In the December 2013 case of *Klayman v. Obama,* Federal District Judge Richard J. Leon ruled that NSA surveillance violated the Fourth Amendment, calling the program an "indiscriminate" and "arbitrary invasion." Leon went further, characterizing the NSA program as "almost Orwellian," in reference to the George Orwell novel *1984* about a world under totalitarian government surveillance.

Also in December 2013, District Judge William Pauley delivered a contradicting verdict, in the case of *American Civil Liberties Union v. Clapper.* In sharp contrast to Leon's ruling in *Klayman v. Obama,* Pauley ruled, citing *Smith v. Maryland,* that metadata collected by the NSA, which is already stored by the phone company, is not protected as the customer has no expectation of privacy with regard to data already "given" or "shared" with the phone company. The EFF and ACLU held that Pauley's decision was a major blow against digital privacy and planned to appeal the decision.

The Intelligence Authorization Act of 2015 (H.R. 4681), passed in March, established guidelines for the storage of data collected through government surveillance.

According to the law, data may only be stored for five years unless the agency in possession can demonstrate a link to terrorism or a potential imminent threat to human life. H.R. 4681 also renews and expands research and development of intelligence technology, including a provision to fund the development of intelligence technology that would allow gathering information from space.

Public Opinion

In a November 2014 Pew Research Report, 91 percent of U.S. adults agreed that consumers lack control over digital information used by companies. In addition, 81 percent of respondents felt that their social media data was not secure, while 46 percent felt insecure sharing personal information via cell phone. A Pew report from March 2015, however, indicated that most Americans have mixed feelings about government surveillance. In general, the study indicated that a slight majority of Americans report being "not very" or "not at all" concerned about government surveillance of cell phones, social media, or other digital communications. However, 61 percent of respondents also said they were increasingly skeptical that U.S. surveillance programs served the public interest. In addition, 60 percent of Americans believed it was unacceptable for the government to monitor "ordinary citizens."

In general, though most Americans disapprove of government mass surveillance programs, most also feel that surveillance will not affect them directly and are therefore largely unconcerned. This lack of concern is largely due to the fact that, as of 2015, there have been few widely publicized cases of the government "abusing" the data that it is collecting on citizens. While privacy advocates argue that oversight and regulation are needed now, to preemptively prevent such abuse, many Americans may remain unconcerned until they have direct proof that modern surveillance is not only invasive but also dangerous *to them*. Revelations of mass surveillance have inspired comparisons to "Big Brother," the symbol of the authoritarian police state in George Orwell's book *1984*. Though few would argue that America has become a repressive regime, the level of data collection currently possible and unregulated is a concern to many precisely because it makes this kind of repression possible.

Micah L. Issitt