THE GREAT COURSES®

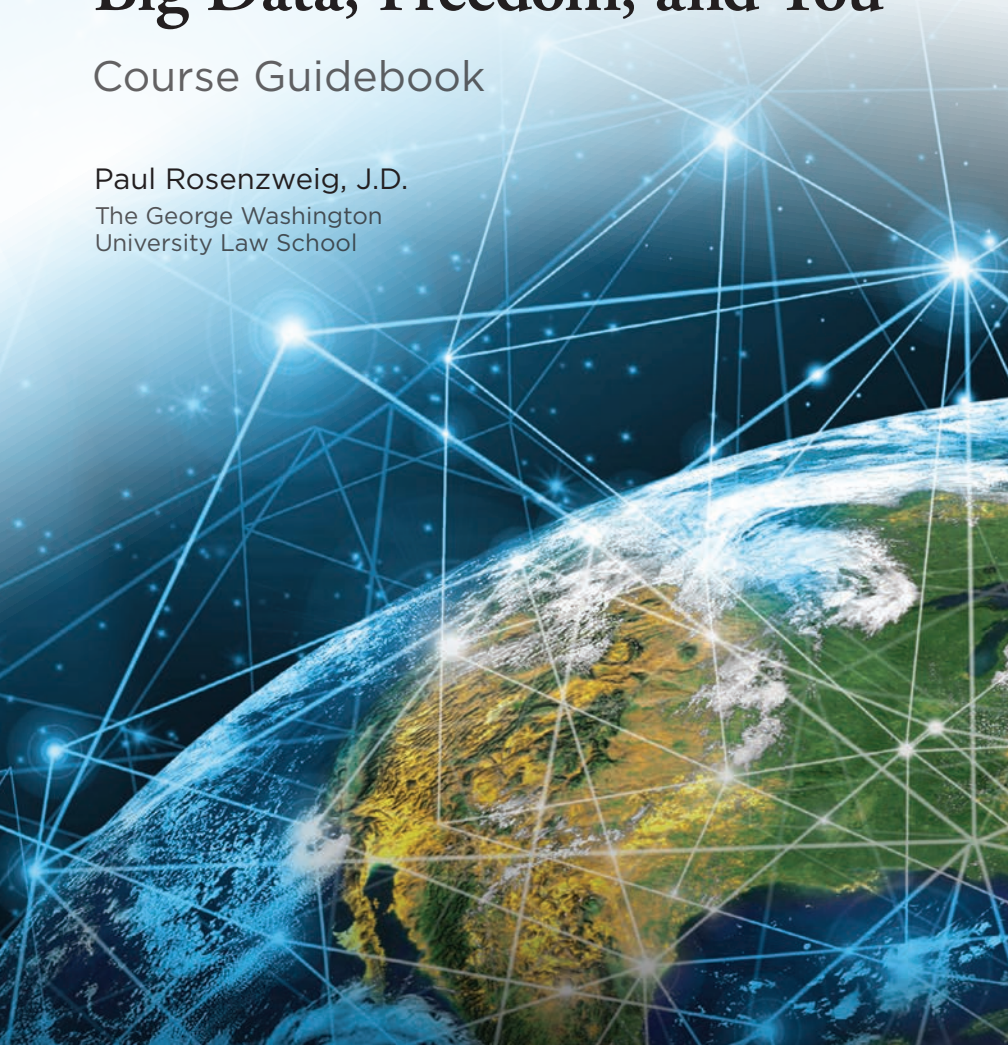
Topic
Professional

Subtopic
Business

The Surveillance State
Big Data, Freedom, and You

Course Guidebook

Paul Rosenzweig, J.D.
The George Washington
University Law School



PUBLISHED BY:

THE GREAT COURSES
Corporate Headquarters
4840 Westfields Boulevard, Suite 500
Chantilly, Virginia 20151-2299
Phone: 1-800-832-2412
Fax: 703-378-3819
www.thegreatcourses.com

Paul Rosenzweig, J.D.

Professorial Lecturer in Law
The George Washington University
Law School

Paul Rosenzweig, J.D., is a Professorial Lecturer in Law at The George Washington University Law School, where he lectures on cybersecurity law and policy. He is a cum laude graduate of The University of Chicago Law School. Mr. Rosenzweig has an M.S. in Chemical Oceanography from the Scripps Institution of Oceanography (a department of the University of California, San Diego) and a B.A. from Haverford College. Following graduation from law school, he served as a law clerk to the Honorable R. Lanier Anderson III of the United States Court of Appeals for the Eleventh Circuit.

In 2011, Mr. Rosenzweig was awarded a Carnegie Fellowship at Northwestern University's Medill School of Journalism, where he continues his affiliation as an Adjunct Lecturer. In 2013, he was the Fifteenth Annual Sommerfeld Lecturer at The Judge Advocate General's Legal Center and School.

In his nonacademic endeavors, Mr. Rosenzweig is the founder of Red Branch Consulting, PLLC, a homeland security consulting company, and a Senior Advisor to The Chertoff Group. He formerly served as Deputy Assistant Secretary for Policy in the U.S. Department of Homeland Security, and he is currently a Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute. Mr. Rosenzweig is a member of the American Bar Association Standing Committee on Law and National Security, a Senior Editor of the *Journal of National Security Law & Policy*, and a Visiting Fellow at The Heritage Foundation.

Mr. Rosenzweig is the author of *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, a coauthor of *Winning the Long War: Lessons from the Cold War for Defeating Terrorism and Preserving Freedom*, and a coeditor of both *National Security Law in the News: A Guide for Journalists, Scholars, and Policymakers* and *Whistleblowers, Leaks, and the Media: The First Amendment and National Security*.

Mr. Rosenzweig's previous Great Course is entitled *Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare*. ■

Table of Contents

The Surveillance State

Big Data, Freedom, and You

Scope

Every day, for good or ill, what you do and what you say is under scrutiny—scrutiny from your friends, your coworkers, and your family, but also from the U.S. government, foreign governments, and large commercial data collectors.

Three trends are driving the growth of surveillance capabilities.

- The proliferation of new sensor platforms. Around the globe, we have new and innovative ways of capturing information and data. They range from license plate readers and citywide television camera systems to drones, biometric identification systems, and other novel ways of collecting data.

- The increased power of data analytics to do correlation analysis of disparate data streams. Powered by Moore's law—the seemingly perpetual doubling of processing capacity—algorithms today can find patterns in immense volumes of data. They often consider billions, if not trillions, of data points as part of the analysis.

- The ever-decreasing costs of data storage. We can imagine a world in which everything is digitized and stored permanently.

The result of all of this is a fundamental restructuring of the relationship between the government and the individual. Technology develops so fast that it outstrips the capability of law and policy to adapt, leaving new surveillance techniques in an ungoverned, lawless domain. Meanwhile, the need for secrecy in some of our surveillance operations makes it difficult, if

not impossible, for citizens to be fully informed about what their government is doing in their name.

But this tension is nothing new. It just gets new expression as technology mutates enduring questions about the balance between the government and the individual.

Since America was founded, we have seen a perpetual and unsteady equilibrium between secrecy and transparency—between security and freedom. The tensions are ineradicable and inherent in the structure of American government. They require us to consider and reconcile two cherished values: limited government and effective government.

This might present a false choice: that you can either have transparency, accountability, and liberty, or you can have secrecy, surveillance, and effectiveness. But the United States can, and indeed does, reflect transparency and secrecy alike—accountability and effectiveness. Our goal should be to maximize both values.

This course explores this dilemma from a number of perspectives. You will learn about some of the history of surveillance, both in America and abroad. You will gain an understanding of how intelligence collection works in the United States and why the 9/11 attacks were so transformative. The course will explore a host of new technologies—from drones to biometrics—and explore their ramifications. You will examine the phenomenon of big data and learn why the Internet is such a treasure trove for spies and commercial companies worldwide. You will explore how some people are trying to get off the grid or make their communications invulnerable. And you will discover how Europe has taken a different approach to answering some of these difficult questions.

In the end, the course will not attempt to "resolve" the fundamental tensions that exist permanently in American democracy. No course possibly could. Rather, the course aims to describe how America is managing them, living with them, and accommodating the competing values to the maximum extent practicable in a time of technological change.

You will explore how, for the surveillance programs that the United States is developing, America—almost uniquely in the world—is struggling with the very difficult and complex question of how to conduct surveillance within the bounds of law. That is a hallmark of the nation's democracy. You also will discover that buried in the legal discourse are more difficult questions about the bounds of policy, ethics, and morality. ■

Security, Liberty, or Neither?

This first lecture will outline the themes that will be addressed throughout this course. First, you'll learn about how technology often trumps the law: In everyday life, legal rules often trail the development and application of technology, and as a consequence, private actors—by introducing new technologies and applications—frequently establish our standards for their use. Second, you'll learn about how the public relies on certain delegated protectors of their liberties rather than rely on themselves. Third, you'll learn about the clash of institutions: Much of what passes for the law is more the product of conflicting institutional imperatives than of legal controls through statutes, regulations, or court decisions.

How Technology Often Trumps the Law

- The first theme in this course is that technology often trumps the law. Part of the struggle to define acceptable surveillance techniques arises from the fact that we are continually trying to apply relatively old laws, and legal interpretatio ns, to relatively new technologies.

- Often, the underlying legislation was written decades ago. In a world in which technology changes as rapidly as it does, it is unreasonable—indeed, almost nonsensical—to expect old laws to fit all new technological applications. Yet, often, that is all we have.

- For example, consider the idea that privacy in cyberspace today and within the government's databases is governed principally by the Privacy Act, which was written in 1974. Although the Privacy Act expresses some important themes and principles that are still applicable today, it's also true that many of them don't fit the current technological capabilities.

- For the most part, law can never catch up with technology; the development of each moves at wildly different speeds. In a democracy, the drafting of each new law moves through multiple layers, from the

private sector (and grassroots of citizen interest) to the public arena (local, state, and federal governments), as well as through multiple levels within the public sector.

- In federal government, we typically start at the top, with the president and Congress, and move from drafting and the passage of new legislation to its articulation and implementation by the federal regulatory agencies—whose methods are inherently slow and deliberate. By contrast, technological change is rapid, and it's only getting faster.

- Moore's law reflects an observation made by the cofounder of Intel, Gordon Moore, about integrated circuits. In the mid-1960s, he noticed that the number of transistors that could fit on a chip doubled every year or two, and he predicted that it would continue to double for the foreseeable future. To date, his prediction has been remarkably accurate.

- Eighteen to 24 months is also a good approximation of the time it takes to get a new law through Congress, when all goes well. And that doesn't count the time it takes for the written regulations that follow, inside the bureaucracy. Technology always seems to move ahead more quickly than laws and regulations do.

- Related to this concern is the inherent conservativism of our legal system. The Supreme Court is always reluctant to address recent technologies with sweeping opinions. Consider *Quon v. City of Ontario, California*, a case from 2010 that addressed the question of whether a police officer had privacy rights to the messages on his pager—a technology that, by 2010, was almost totally out of date.

- While the Court addressed employer-provided communication devices, a broad-brush technology that could have widespread implications, it also provided a narrow view of the issue. It was reluctant to rush ahead of technology, stating, "At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve."

- A related aspect of the disconnect between the pace of law and the pace of technology that you also will explore in this course is the role of private sector actors in creating expectations of privacy and in defining the role of surveillance technology.

- After all, almost all of the technologies that will be covered in this course—including tools like drones and traffic cameras and the GPS in your car—are manufactured by private corporations. Consequently, because private companies bring us most of today's new commercial technologies and applications, they also have the initial responsibility for setting the rules on the collection, storage, use, and analysis of data that the new technology captures.

- Often, we find that those private sector guidelines and choices are much more important in determining whether, when, and how your privacy and civil liberties will be invaded than are any rules promulgated by the government.

- Of course, that's not always true. When the government purchases or invents a piece of new technology—or when it buys data and information from the private sector and then uses it for its own purposes—the question quickly becomes one of governmental rules and controls.

- Who sets the terms for how the government uses the system? Typically, it is Congress, through legislation, or the executive branch, through its internal policy and guidance. Sometimes, in the case of conflict, it might be the courts.

- Nonetheless, at least in the first instance, private actors, who are by no means representatives of the general populace, make many decisions that directly affect how surveillance is accomplished. Unlike elected officials, these private actors take their cue not from voters but from consumer-driven demands and concerns. It is, therefore, an oddity that much of what we consider to be issues of great public policy concern in the surveillance space are, in the first instance, shaped by private actors.

The Supreme Court of the United States

Delegated Control

- The second major theme is the idea of delegated control—a system that reflects how transparency and secrecy are in continual tension.

- We want to exercise oversight of our secret intelligence operations, such as the Central Intelligence Agency (CIA) and the National Security Agency (NSA). Oversight is fundamental to democracy, and transparency is essential to oversight. You can't control what you can't see. But we also understand that complete transparency—exposing all of their activities to public scrutiny—would frustrate their effectiveness.

- Methodologies and sources developed by our intelligence community often cannot be publicly disclosed without draining them of all usefulness. That's a conundrum in a democracy: We want to maintain

public control of our agencies, but we also want them to be effective at what they do.

- Another theme that will be examined in this course is the idea that the American public has delegated to its representatives in Congress and the courts some of the responsibility for overseeing the intelligence community. Something of this nature is, to many Americans, an essential method of auditing surveillance activity without disclosing it. However, today many think that this model of delegated transparency is outmoded and ineffective. Especially in light of recent revelations about NSA surveillance of Americans, some think that the current system is too insular.

The Clash of Institutions

- The final overarching theme in this course is the idea that policy and law are created by the clash of institutions every bit as much as they are by formal legal processes. Often, these are conflicts between branches of government—between, for example, the executive branch and the legislative branch, or between either of them and the judiciary branch.

- Beyond this, there are often conflicts even within the executive branch—between, for example, the White House and the intelligence community, or between the Department of Justice and the Department of Homeland Security. And sometimes one part of the government is in tension with private sector actors, who march to a different motivational drummer.

- Standing in lonely opposition, in some ways, to the government and even the private sector on issues of surveillance law and policy is civil society. Throughout this course, you'll discover how nongovernmental organizations and advocacy groups exert a large influence on the development of surveillance law and policy, as well as its application. These include formal organizations, such as the American Civil Liberties Union, as well as informal citizens groups and small communities, which might, for example, simply oppose the flight of drones over their own houses.

- Finally, you'll learn about the role of independent journalism in monitoring surveillance activity on behalf of the public. The press, or media, is sometimes called the fourth estate because it has an outsize role in defining the debate and, to some degree, resolving it.

Questions to Consider

1. Which is preferable: rules and guidelines set by common practice or by legal rules? Do you think it is realistic to try and set rules in a dynamic technological environment?
2. How significant do you think the Comey/Mueller threat to resign really was? Does that sort of pressure work on presidents?

The *Charlie Hebdo* Tragedy

This lecture will use the *Charlie Hebdo* events to frame some questions about how the surveillance state can, and should, operate. First, you'll learn about the *Hebdo* attack in the context of the challenges that surveillance agencies face. Next, you'll learn about the several types of surveillance, including physical surveillance, electronic surveillance, and "dataveillance." Finally, you'll discover the possible uses—and abuses—of surveillance by learning about two polar cases: the hunt for Osama bin Laden and the routine scrutiny of air passengers by the Transportation Security Administration.

The Attack on *Charlie Hebdo*

- January 7, 2015 marks the date of the horrific terrorist attacks in Paris that killed 12 people, including eight journalists at the *Charlie Hebdo* magazine. Two Islamic jihadists named Said and Cherif Kouachi stormed into an editorial meeting of the magazine staff. Their objective was to exact revenge against cartoonists employed there who, in their judgment, had blasphemously mocked the prophet Mohammed.

- Dressed like soldiers and armed with assault rifles, the two brothers killed the journalists, two police officers, a maintenance worker, and a visitor to the French satirical weekly newspaper. They injured 11 more people before leading French counterterrorism forces on a 72-hour chase. Ultimately, they were cornered and killed during a shootout in northeast Paris.

- Meanwhile, another Islamic sympathizer, Amedy Coulibaly—who might or might not have coordinated his activities with the Kouachi brothers—took hostages at a kosher supermarket in Paris, where four more innocent Parisians died before he, too, was gunned down.

- The world reacted in shock and anger. Twitter, Facebook, and Instagram exploded with the "*Je suis Charlie*" hashtag and photos. The people of France marched in solidarity with the cartoonists. World leaders flocked to Paris in demonstrations of support. And the next issue of *Charlie Hebdo* was translated into more than 16 different languages, publishing more than 3 million copies, which sold out in short order. The assault on free speech and free expression proved unavailing.

- But in the wake of the *Charlie Hebdo* tragedy, many questions emerged about the failure of the French surveillance system. At least one of the Kouachi brothers, Said—and possibly both of them—had taken weapons training in Yemen and interacted there with senior leaders of al-Qaeda in the Arabian Peninsula, a group often identified as AQAP. By some accounts, Said Kouachi met with Anwar Awlaki, the American-born sheik who later died in an American drone attack. The younger brother, Cherif, in an interview while still cornered, claimed Awlaki had financed the Paris attack.

- The Kouachi brothers were not unknown to the French antiterrorism forces. Cherif had been arrested by French authorities in 2005 as he was about to leave to fight in Iraq. He was convicted of supporting terrorism and sentenced to three years in prison for recruiting fighters to join the notorious leader of the al-Qaeda affiliate in Iraq, Abu Musab al Zarqawi. But Cherif didn't serve any time after the conviction. The judge ruled that his pretrial detention had been enough.

- Likewise, Amedy Coulibaly was said to have been on a U.S. terrorist watch list for quite a while before the attacks. There were also, it appears, records of his travel to Syria and a video he made declaring loyalty to the Islamic State.

- After *Charlie Hebdo*, the French intelligence services faced some of the same questions that recur after any terrorist incident, including questions about intelligence failures. With that kind of background, how is it that the Kouachi brothers went unobserved? The failure is magnified when we learn that at least one of them had been under surveillance until six

Rally after the *Charlie Hebdo* tragedy

months before the attack and that he actually had been downgraded as a threat. But even with all of that intelligence, we somehow missed the plot.

- Were we doing enough? Were we doing too much of the wrong thing? In fact, does surveillance work at all? Can surveillance programs be conducted in a way that fosters freedom and respects privacy and civil liberties while still being effective? If so, how?

- *Charlie Hebdo* is a forum for expressing free speech. It would be a cruel irony if the same steps that France took to protect the magazine ended up chilling the magazine's freedom of expression. The attack captures the "damned if you do, damned if you don't" nature of the problem of security and surveillance.

Types of Surveillance

- Surveillance comes in three basic forms. First, there is physical surveillance, dating from the times of Alexander the Great and earlier up to the Stasi state in post–World War II East Germany. This is the

traditional form of scrutiny that has always been the province of spies and intruders.

- For hundreds of years, this potentially wide-ranging form of physical surveillance was the only sort of surveillance we knew. It morphed slightly over time as the nature of our physical environment changed. Eventually, as the means of communication changed, so, too, did the means of interception.

- American "signals interception" (another name for electronic surveillance) came of age during the Cold War. Some of the surveillance seems, in retrospect, remarkable for its value. It is said that for years, the CIA ran a joint electronic surveillance operation with the Chinese in the western deserts of China to monitor Soviet missile launches. On the other hand, the Cold War also saw some signs of governmental abuse, the likes of which we've more recently come to be concerned about again.

- To these traditional forms of surveillance, we add a third: the collection, and analysis, of personally identifiable data and information about individuals. "Dataveillance" is an inevitable product of our increasing reliance on the Internet and global communications systems. We leave an electronic trail almost everywhere we go.

- In a networked world, technological changes have made personally identifiable information pervasively available. And as the available storehouse of data has grown, so have governmental and commercial efforts to use this data for their own purposes. Commercial enterprises target ads at consumers and solicit new customers. Governments use the data to identify and target previously unknown terror suspects.

The Hunt for Osama bin Laden

- The hunt for Osama bin Laden used all three forms of surveillance, often in overlapping and mutually supporting ways. The entire story is not fully declassified, but what we know of it from public reports suggests that the United States used almost every means available to track down the terrorist mastermind.

- The key to finding bin Laden appears to have come from identifying, and then tracking, one of his couriers. Initial information regarding the courier was collected from war-on-terror detainees at Guantánamo Bay. They gave American intelligence the courier's pseudonym: Abu Ahmed al-Kuwaiti.

- We were told that al-Kuwaiti was a protégé of the Pakistani senior leader of al-Qaeda, Khalid Sheikh Mohammed. It was not, however, until 2009 that we learned that the courier lived in Abbottabad, Pakistan. To track him, the CIA initially used sophisticated geolocation technology that helped pinpoint the courier's cell phone location.

- Eventually, that allowed the CIA to determine the exact type of car that Kuwaiti drove (a white SUV). Using physical and electronic surveillance, the CIA began tracking the vehicle. One day, a satellite captured images of the SUV pulling into a large concrete compound in Abbottabad. Agents determined that al-Kuwaiti lived there, and they used aerial surveillance to keep watch.

- The residents of the compound were extremely cautious. All communications to the outside world ran through al-Kuwaiti and his brother, who came and went from the compound. Another man, who lived on the third floor, never left. He stayed inside the compound, and underneath a canopy, frustrating overhead satellite surveillance. Some analysts speculated that this was bin Laden.

- In addition to satellites, the government flew an advanced stealth drone, the RQ-170, over Pakistan to eavesdrop on electronic transmissions from the compound. To get a better sense of activity at the compound, CIA spies moved into a house on a property next door. Surveillance also played a role in planning the eventual Navy Seal assault on the compound.

The TSA No-Fly List

- A common form of post-9/11 surveillance is the Transportation Security Administration's (TSA) airport screenings. By now, most Americans

Airport security checkpoint

are pretty familiar with the long lines, thorough pat-downs and X-ray inspections that are part of the process.

- But that physical screening comes at the back end of a process that begins much earlier, when you first make a reservation to fly. TSA security directives require airline passengers to present identification when they make a reservation. Later, if you are selected for secondary screening, you and your bags will be taken out of line for additional scrutiny.

- A passenger's name, gender, and date of birth are used for a form of dataveillance screening known as Secure Flight. The passenger's information is checked against a terrorist-screening database that contains a list of individuals who are identified as persons of interest by the U.S. intelligence community and are considered potential threats to American national security.

- The Secure Flight program has not, as far as is publicly known, ever spotted a terrorist. It has identified a number of criminals attempting to

travel, and physical screenings often uncover people who are trying to smuggle goods or guns onto a plane. But there are some who consider the costs of such pervasive surveillance excessive in relation to its benefits.

Questions to Consider

1. Are we setting up the government for an impossible task? Is it reasonable to expect that we will never have a terrorist attack again?
2. Is it feasible for Stimson to be right—that nations should not spy on each other? How would such an agreement be verified? And if not, then what is the alternative?

East Germany's Stasi State

The subject of this lecture is the Stasi surveillance state of East Germany. First, you'll learn about the Nazi precursor to the Stasi system. Against this background, it is easy to see how surveillance came to pervade Communist East Germany after World War II and why contemporary Germans so highly value privacy and limits on state surveillance. Next, you'll discover how Stasi surveillance functioned. The lecture will close with a short consideration of why (if at all) the Stasi history is relevant to contemporary debates.

The Nazi Precursor to the Stasi System

- Prior to the Cold War standoff between Eastern and Western Europe, there was significant state surveillance in Germany during the Nazi régime leading up to—and throughout—World War II.

- Nazi surveillance was undergirded by one of the most sophisticated data collection and analysis systems of the time. It was possibly the first systematic use of "dataveillance" by a nation state. The system was developed and operated by a company known as Dehomag, the corporate acronym for *Deutsche Hollerith Maschinen Gesellschaft mbH* (German Hollerith Machines LLC).

- Dehomag was a subsidiary of the U.S. technology company IBM. It had a monopoly on data analysis for the German government in the years leading up to, and during, World War II. The "Hollerith" in the corporate name was Herman Hollerith, a German American inventor who developed a method for instructing the analog data accumulators of that era through the use of punch cards.

- Hollerith first invented and used his data punch cards to capture the data for the 1890 U.S. Census. He founded the Tabulating Machine Company in 1896, which in 1924 became known as the International

Business Machines Corporation (IBM). During the Nazi era, IBM punch cards were used to compile data on Jewish citizens in Germany as part of the German census.

Stasi Surveillance

- The internal security force for the German Democratic Republic, also known as East Germany, was known as the *Ministerium für Staatssicherheit* (Ministry for State Security)—commonly known as the Stasi. Many commentators describe it as the most repressive, and oppressive, surveillance system ever operated.

- The following are some of the activities that Stasi undertook during its heyday.
  - It had a system for monitoring telephone conversations.
  - It also had what is known as a "mail cover" system that opened up letters and parcels coming in from overseas, as well as mail to certain targeted people.
  - It tracked all of the few foreigners who were allowed into East Germany.
  - It had a division whose job it was to detect whether any citizens had illegal Western foods in their garbage.

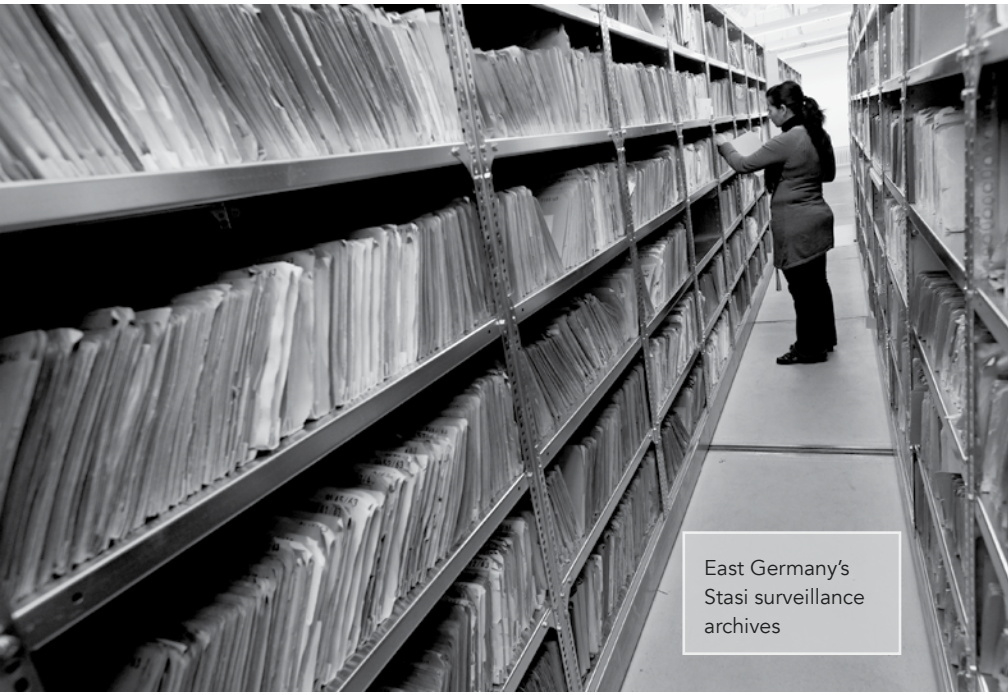
- What distinguished Stasi from other surveillance systems was the massive number of its informants. In Germany, they were known as informal collaborators, or *Inoffizieller Mitarbeiter* (IMs). Although estimates vary, we can say with confidence that in 1989, on the cusp of the fall of the Berlin Wall, the East German government employed more than 170,000 of these IMs.

- When you consider that the entire population of the country was only 16 million at the time, this means that more than one percent of the population served as informants. And if you exclude the very young and the very old, it is likely that as many as two percent of the population

of adult age were IMs. Perhaps worst of all, about 10,000 of these informants were younger than 18. They were children, many of them, perhaps, spying on their parents.

- Nazi hunter Simon Wiesenthal believed that the Stasi were even more oppressive than the Nazi Gestapo. Even if we don't count the informants, the Stasi workforce was larger, on a per capita basis, than the Gestapo or the Soviet KGB.

- One of the most insidious forms of Stasi surveillance went by the name *zersetzung*, a form of psychological harassment that was designed to wreak havoc on an individual without any need to arrest or torture the target.



East Germany's Stasi surveillance archives

- Some of these techniques were semi-overt: The Stasi would arrange, for example, for your work to go poorly. Although the causes might not be known to the subject of the attack, the effects were pretty evident. Other techniques were more insidious. It would sometimes, for example, spread rumors about a target among his or her friends and colleagues—stories of alcoholism, parental neglect, or the like.

- Sometimes, the Stasi would play mischievous mind games with a target. They might, for example, enter his or her house and move the furniture around, or they might change the time on an alarm or replace tea bags with different types of tea.

- Other tactics were similarly abusive. Reports exist of the Stasi arranging for a target to get deliberately incorrect medical treatment or to receive doctored photographs purporting to show him or her in a compromising situation.

- The Stasi used *zersetzung* for a number of reasons. First, there is the in terrorem effect of the technique: The victim doesn't know what is happening. The mystery makes the adverse situation all the more difficult. And everybody around the target can watch as he or she crumbles under the relentless pressure of state harassment.

- Second, *zersetzung* is efficient. Holding someone in a cell is expensive; harassing them every third day is much less so. And it is effective.

- Finally, an added advantage of psychological operations was their deniability. The Stasi could plausibly say that it had no idea about what was happening and thereby allow the East German regime to maintain a false facade of international respectability.

- After the fall of the Berlin Wall, the Stasi tried to destroy many of its files. They were thwarted only when East German citizens stormed the offices and stopped them from expunging the records. Perhaps only 10 percent of the records were destroyed—nobody knows for sure.

- According to the German magazine *Der Spiegel*, the surviving files occupy more than 100 kilometers (roughly 62 miles) of shelf space. In addition, there are 16,000 sacks of shredded documents that some are trying to reconstruct. That's a huge record of human conduct, from the trivial to the significant.

- On the other hand, not everybody was in the system. Since the fall of the Berlin Wall, nearly 3 million Germans have asked to see their files. And somewhat surprisingly, roughly 50 percent of those who make the request don't have a file on record with the Stasi.

- The Stasi system was not the only one of its kind. Chinese surveillance (what little is known of it) looks very much like that employed by the Stasi. Today, for example, it is standard practice for American businesses to warn their traveling employees not to take along their personal electronics and to destroy the phones they do take along upon returning to the United States. Indeed, the intelligence hierarchy in China is sufficiently obscure that almost nobody knows which agency is in charge of domestic surveillance or how many citizens are under scrutiny.

The Relevance of Stasi History to Contemporary Debates

- At this point, now that you understand the Stasi system, it is fair to ask why, in a course on the modern surveillance state, our discussion began with the consideration of the Stasi? After all, they've been gone for more than 25 years. What does distant history have to do with today?

- The choice could be defended on any number of grounds. First, 25 years is not so long ago. American policy still revolves, in part, around events that occurred in the 1960s and 1970s. So, one answer is that a page of history is worth a volume of logic. On that basis alone, the history of one of the most intrusive surveillance systems is worth studying.

- But the better answer is that for good or ill, the Stasi system has become a sort of benchmark in political discourse for the description of systems of surveillance, and one that is deployed with some regularity. For example, Markus Ferber, a member of Chancellor Angela

Merkel's Christian Democratic Union, once assailed the United States for "American-style Stasi methods." *The Nation* magazine also has bemoaned the United States as "A Modern-Day Stasi State." And not long ago, in lights on the walls of the U.S. embassy in Berlin, a German artist projected the message "United Stasi of America."

- When President Obama defended previously undisclosed methods of the National Security Agency activity, he cited East Germany as a "cautionary tale of what could happen when vast, unchecked surveillance turned citizens into informers and persecuted people for what they said in the privacy of their own homes." Of course, he was using the Stasi as a counterpoint, answering accusations against the NSA by saying that it was not a similarly vast, unchecked effort to collect data.

Questions to Consider

1. What do you think of the comparison between the Stasi and the United States today? Is it apt, or is it overwrought?
2. The use of IBM technology in Nazi Germany is just the first instance we will see of tools being put to malicious uses by an ill-meaning government. What responsibility, if any, do manufacturers bear for how their products are used?

Surveillance in America

In East Germany, the Stasi internal security apparatus advanced the Communist Party's interests over those of individual citizens. What can a liberal Western nation do to prevent that sort of repression from occurring? America faced this question during the early 1970s, when the U.S. government was discovered to have engaged in illegal and often-immoral surveillance activities. Scrutiny focused on the CIA, the NSA, and the FBI. As the revelations grew, public concern became so acute that Congress and the executive branch each undertook extensive reviews. In the end, the entire structure of federal covert operations was transformed. This lecture is the story of that transformation.

Surveillance in America

- In the 1950s, in the immediate aftermath of World War II, Americans were afraid of Communism and vigorously defended themselves against the slightest hint of it. Today, we rightly look back with a mixture of shame and disdain at one of the most virulent forms of that pursuit: the anti-Communist rants of Senator Joseph McCarthy and the mole-hunting inquiries of the House Un-American Activities Committee (HUAC).

- But the excesses of people like the late Wisconsin Senator Joseph McCarthy are often mistaken for the underlying motivation of all who serve in government. And that is plainly incorrect. One recurring theme we see, over time, is the idea that most, though certainly not all, individuals who work within the U.S. intelligence community are motivated by a heartfelt concern for national security. Indeed, without in any way defending McCarthyite excess, it is useful to understand what was driving the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) during the 1950s and 1960s.

- The world had just seen the Soviet coup in Czechoslovakia in 1948, the fall of China to Mao Zedong in 1949, the Korean War beginning in 1950, and the Soviet Union's successful detonation of an atomic bomb—largely on the back of its own espionage operation.

- Meanwhile, the United States and the Soviet Union had failed to reach a postwar settlement that would allow for amiable coexistence. Most American policymakers—including presidents Truman, Eisenhower, and Kennedy—saw the Soviet Union as intent on controlling as much of the world as it could.

- And in the late 1940s and early 1950s, a series of espionage incidents seemed to confirm this view. One of the earliest was the discovery, in 1945, of thousands of classified government documents in the offices of *Amerasia*, a magazine with ties to the Communist Party of the United States of America.

- The era also saw the investigation into whether a former top U.S. diplomat, Alger Hiss, was secretly a Communist; the prosecution of a U.S. Department of Justice official named Judith Coplon, who allegedly was a KGB spy; and the still-historically-controversial arrest and execution of Julius and Ethel Rosenberg, after their convictions of conspiring to spy for the Soviet Union.

- None of this excuses the unwarranted, and often illegal, activities undertaken by the intelligence community in its anti-Communist fervor. With the benefit of perfect 20/20 hindsight, we can see this historical vision as hysteria motivated by fear. And perhaps from that we can learn some lessons for today. But calling it unreasoning hysteria does not lessen the urgency with which the fear was felt.

The Church, Pike, and Rockefeller Committees

- Armed with that background, let's examine some of the abuses and excesses of the American intelligence and law-enforcement communities in the years leading up to the mid-1970s. The issues first started coming

The Federal Bureau of Investigation in Washington DC

to light in the early 1970s through investigative reporting that revealed illegal activities involving the American intelligence community.

- In 1970, Christopher Pyle—a former Army captain—disclosed a domestic spying program conducted by the Army itself. Then, in 1974, Seymour Hersh, an investigative reporter for *The New York Times*, published details of several CIA operations that exposed activities ranging from covert efforts to subvert foreign governments and to intelligence activities within the United States aimed at political opponents of the executive branch.

- These revelations led the House and Senate to independently charter two select committees responsible for thoroughly examining how America's intelligence and law-enforcement communities had conducted themselves.

- Long Island Congressman Otis Pike chaired the House committee. Idaho Senator Frank Church chaired the parallel committee in the Senate—hence the name "the Church Committee."

- In addition, in 1975, President Gerald Ford asked Vice President Nelson Rockefeller to lead an internal investigative review by the executive branch, an inquiry known as the Rockefeller Commission. Over the course of the next two years, these three panels worked at a frenetic pace.

- Congress, through its investigating committees, had the principal role in reforming the intelligence community. The courts also played a complementary role in the effort. The leading case is titled *United States v. United States District Court*, sometimes referred to as the *Keith* case, in which the court limited its holding to domestic surveillance and said that different rules might apply when the surveillance occurred outside the United States or was directed at a foreign power or at non-Americans.

- There is little that can be said in support of the illegal domestic-spying activities by our intelligence and law-enforcement agencies. At the outset, perhaps those who instituted them thought they were doing so for valid reasons. But as the surveillance programs morphed, they became increasingly divergent both from their original justifications and even from any practical reality.

- The real value in the authoritative, constitutional, and reasoned reviews of the Church, Pike, and Rockefeller committees is that, through their diligence, they exposed unlawful and unregulated intelligence and law-enforcement activity. And the result—stricter oversight—was a triumph for democratic principles. These committees put in place a new system of oversight and control that continues, largely intact, to this day. It represents a meaningful effort by democratic institutions to exercise oversight and maintain intelligence and law-enforcement activities within the bounds of law.

New Structures of Oversight and Control

- In the wake of their investigations, the Church and Pike Committees took on the full-time job of exercising oversight of the intelligence community. Senate Resolution 400 in 1976 and House Resolution 658 in 1977 established two intelligence committees as permanent select committees that continue to function to this day. The two committees were seen as an essential component reigning in the unregulated intelligence community.

- By law, Congress must be kept "fully informed" of significant intelligence activities. Often, this means providing notification of covert action to the Congress in the form of notification to the intelligence committees. Sometimes, that notice might be delayed until after a covert action has taken place.

- Although the two congressional committees have exercised some degree of control over the intelligence community, many dispute how much control they really muster.

- Through the mechanisms of congressional hearings, consideration of presidential nominations, and the authorization and appropriations process, the intelligence committees exercise day-to-day reviews of the intelligence function.

- Many top leaders of our intelligence and law-enforcement agencies—including all of the senior leaders of the Department of Justice, the FBI, the Director of National Intelligence, and the head of the CIA—are subject to senatorial confirmation.

- That requirement has developed into a form of congressional oversight of surveillance activities. In recent years, for example, Congress has increasingly come to withhold confirmation until the executive branch provides it with additional information that relates to areas of congressional oversight and inquiry.

- Congress also can legislate limits on intelligence-community activities through budgetary authorizations, and appropriations—that is, by funding or declining to fund particular intelligence activities. In more extreme circumstances, full-scale investigations have been undertaken.

- Meanwhile, Congress also sought to address the fact that foreign surveillance might not be subject to judicial review under the Constitution. To fix that problem, in 1978 Congress adopted the Foreign Intelligence Surveillance Act (FISA), which defines the procedures and processes for authorizing the physical and electronic surveillance of foreign powers and agents of foreign powers.

- Under FISA, the government was authorized to conduct surveillance relating to foreign intelligence matters that might also include surveillance of American civilians acting as agents of a foreign power if—and only if—court authorization was obtained first.

- And that authorization would be given only if the court found that there were probable cause to believe that the target of the investigation was in fact a foreign power or an agent of a foreign power. In addition, if the target of the surveillance were a U.S. person, there also had to be probable cause to believe that the person's activities might involve espionage, or other similar conduct, in violation of the criminal statutes of the United States.

- At the same time, because such matters under investigation would be highly classified, Congress chose to create a special court called the Foreign Intelligence Surveillance Court (FISC), where the government is able to present its evidence justifying surveillance in an ex parte manner. ("Ex parte" means a decision that a judge makes after hearing only one side of the case.) The FISC proceedings are also conducted behind the veil of classification, such that its decisions are typically not recorded or published for public consumption.

- Two things are notable about these new mechanisms. The first is that they are pretty unique globally. Almost everywhere else in the world,

intelligence collection is exclusively the province of the executive. The United States has a shared-governance model. We are fortunate to have the oversight system we have.

- Second, these new systems of congressional review and judicial review take place in a delegated, or semitransparent, manner. Covert activities that previously were not subject to review outside of the executive branch are now subject to review, behind closed doors, by a subset of our elected congressional representatives—and, in a non-adversarial process, before federal judges—all of whom we expect to pass on the legality and propriety of the surveillance activities being undertaken.

- This is halfway between the complete secrecy that characterized surveillance activities in the early Cold War era and the complete transparency that some people view as preferable.

Questions to Consider

1. The lecture has painted the Church and Pike Committee investigations as successful assertions of democratic control over the intelligence community. Were they? Or are the reforms they initiated more window dressing than effective controls?
2. We described a system of congressional and judicial oversight as a substitute for complete transparency. Can you think of any alternative structures that might work better?

Failing to Connect the Dots on 9/11

In October 1978, President Jimmy Carter signed into law Foreign Intelligence Surveillance Act legislation that established a new framework for American policy, mandating a strict separation of the CIA and the FBI—or, more broadly, between criminal law and espionage. In effect, the Congress erected a "wall" between intelligence gathering and law enforcement after the Senate Church Committee uncovered Cold War–era abuses in U.S. intelligence agency practices. The new law was a procedural mechanism to restrain the surveillance state. Did this wall imperil—rather than protect—American democracy in September 2001? Some think so, but others have their doubts.

The Wall

- The wall stems from an era when legal, social, and bureaucratic restraints on communications between the intelligence sector and law enforcement were thought to be an important limit on governmental intrusion. Foreign Intelligence Surveillance Act (FISA) legislation—in the years before the terrorist attacks, but after Congress uncovered a string of errors and abuses in the intelligence sector that encroached on citizens' rights—strengthened the barrier between intelligence and law-enforcement communications to abate such errors and excesses.

- Why does the wall matter at all? Or, why is there value in separating law-enforcement methods from intelligence activities? The answer lies in the different procedures and forms of inquiry that they use.

- There is a clear distinction between criminal investigations, which are typically conducted under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (known as Title III investigations), and national security investigations conducted under FISA. The latter—relating to national security—provides considerably more deference to the executive branch at every step.

U.S. President
Jimmy Carter
(1924–)

- For example, while Title III and FISA alike require government officials to obtain ex ante permission from judicial officers for electronic surveillance, courts under Title III (that is, criminal law enforcement) impose a far stricter standard of review before granting authorization.

- Furthermore, after the surveillance is complete, aggrieved parties under Title III who say that the government made an error have substantial rights to challenge the government's conduct. These rights are nonexistent in the FISA regime.

- Under Title III, the fruits of electronic surveillance can be used in a prosecution only if the defendant is first given copies of the government's application and the court order approving the surveillance. FISA applications, on the other hand, are generally not disclosed unless ordered by the Foreign Intelligence Surveillance Court (FISC), which is limited as to when it can order disclosure.

- As a practical matter, defendants in criminal actions rarely have access to FISA applications. Even evidence relating to defendants under investigation for simple domestic crimes, such as drug smuggling, for example, might sometimes be discovered as a collateral part of an intelligence investigation. When that happens, however, the accused drug dealers will usually not understand why it is that the government got the authorization to conduct surveillance in the first instance. The application remains cloaked in FISA's secrecy blanket.

- An earlier Supreme Court decision in the *Keith* case, which pitted security concerns against civil liberties during the administration of President Richard Nixon, found that domestic surveillance—whether for criminal or national security reasons—had to fully satisfy the warrant requirement of the Fourth Amendment. The Fourth Amendment prohibits unreasonable searches and seizures and requires any warrant to be judicially sanctioned and supported by probable cause.

- But implicit in this requirement for domestic surveillance is the idea that surveillance of a foreign national for national security purposes

might be subject to a less-stringent "reasonableness" standard. Courts around the country soon agreed, holding that surveillance for foreign intelligence purposes needed to be reasonable (but might not require a warrant).

- How do you make such a distinction—between domestic criminal and foreign intelligence activity? Information doesn't come with a sign on it that says "use me only for foreign intelligence purposes." And once you collect information, it becomes difficult to deliberately forget it.

- What if, during the course of surveilling a Russian spy, the CIA discovers information about a Russian drug ring? Does it close its eyes to that, or does it share with the FBI? To answer, the courts have developed something that has come to be known as the "primary purpose" test: The lawfulness of surveillance would be determined by the intent, or purpose, of the investigation. If it were for foreign intelligence, then FISA procedures applied. If it were for anything else, the government had to apply the more stringent Title III rules.

- Some Justice Department officials used the same logic to prohibit consultations and coordination among intelligence and law-enforcement agents and prosecutors. They were afraid that federal courts might look at coordination between law enforcement and the intelligence community and think that they were impermissibly using the relaxed FISA rules to collect evidence for a criminal case.

- The more such consultations occurred, or the more FISA was used to obtain evidence for a criminal prosecution, the more likely courts were to find an improper purpose, they believed. So, they decided that we needed rules limiting consultation—sort of a preemptive strike against being accused of an improper purpose.

- In July 1995, President Bill Clinton's attorney general, Janet Reno, approved coordination procedures that "applied in most cases." As prominent national security lawyer Scott Glick says, "The guideline limited contacts between the FBI and the Justice Department's Criminal

Division, in cases where FISA collection was taking place, in order to 'avoid running afoul of the primary purpose test used by some courts.'"

- On their face, these procedures were stringent: They were meant to limit, but not prohibit, the coordination of intelligence and law-enforcement activity. In practice, they seem to have been interpreted (some say misinterpreted) as a strait jacket.

- As Glick rightly summarizes: The "foundations of the FISA wall lie in the 'primary purpose' test." The Department of Justice (DOJ) acted as a barrier to communications so that it could tell the court that a wall existed. In other words, the wall was a procedural barrier that made it impossible to use intelligence for law-enforcement purposes—and therefore allowed the Office of Intelligence Policy and Review (OIPR) to reassure the courts that intelligence collection was exclusively for intelligence purposes.

- One critical procedural aspect of the rules was the requirement that specialized requests for surveillance had to go through FBI headquarters and the OIPR at Main Justice. OIPR was both the wall and a gatekeeper—making sure that the FBI just didn't talk to the CIA, and vice versa.

- Why? What could account for this attitude? Some can rail against ignorance or malfeasance, but the likely answer is more prosaic. The creation of the wall, and rules about it, erected a compliance culture within the FBI and DOJ, where failure to follow procedure resulted in adverse personnel actions.

The 9/11 Commission

- The congressionally authorized 9/11 Commission reviewed the function of the wall prior to the terrorist attacks and painted a depressing picture of bureaucratic rigidity: "Over time," the commission report concludes, the OIPR and the FISC "began to see mere contacts between the FBI and the Criminal Division as a proxy for improper direction and control. Significantly, OIPR viewed its role primarily as an officer of the FISA Court and therefore responsible for stewardship of the court's responsibilities.

9/11 Commission Members

It viewed its role as an advocate for its institutional clients [that is, the FBI] as secondary."

- In November 2000, the FISA Court added a requirement that no one in the FBI or DOJ—including persons working solely on intelligence investigations—could see FISA material before signing a form acknowledging that they understood the restrictions on sharing any information they obtained.

- This form assured that information sharing would essentially come to a halt, because agents feared that they would lose their jobs if they shared any intelligence information with criminal investigators. Although this "wall" of restriction formally applied only to FBI intelligence collection, it also came to be adopted by other intelligence agencies, again out of an overabundance of caution.

- Part of what the 9/11 Commission said about that phenomenon is as follows: "The National Security Agency (NSA) also placed restrictions on

the sharing and use of information it collected. Initially these restrictions merely governed the use of its reporting in criminal matters. In December 1999, however, the NSA began placing new, more restrictive caveats on its bin Ladin–related reporting. These caveats precluded sharing the information contained in these NSA reports with criminal prosecutors or investigators without obtaining OIPR's permission."

- The NSA couldn't always tell exactly what source it had gotten information from—a restricted FISA source or an unrestricted non-FISA source. Because of this, in the run-up to 9/11, the agency concluded "that there was no administratively easy method to determine which of its reports were from FISA-based collections," according to the 9/11 Commission. "Thus, caveats were added to all NSA counterterrorism reporting that precluded sharing the contents of the reports with criminal investigators or prosecutors without first obtaining permission from NSA's general counsel."

- Consider, for example, what happened to the agency's surveillance of two of the 9/11 bombers. As the 9/11 Commission tells us, "In December 1999, the NSA picked up the movements of Khalid al Mihdhar, an individual then identified as Nawaf Mihdhar, which linked him to a terrorist facility in the Middle East. Mihdhar was tracked to Kuala Lumpur, where he met with other then-unidentified individuals. Some photographs were taken of these men on the streets of Kuala Lumpur. The surveillance trailed off when three of them moved on to Bangkok, on January 8, 2000."

- Those pictures became relevant to the FBI's pre-attack criminal investigation in July 2001. Unfortunately, as the 9/11 Commission found, the NSA reports contained caveats that their contents could not be shared with criminal investigators without the OIPR's permission.

- The failures of 9/11 were less about statutory language and more about human fears and hesitations—an abundance of caution and the inability of bureaucratic organizations to adapt to discrete circumstances. Even

more than a wall, the law created a space—a dangerous void—between the government's criminal and intelligence sides of the house.

The Aftermath of 9/11

- The reaction after 9/11 was swift. In late September 2001, the executive branch sent Congress draft legislation proposing changes to FISA's certification requirement for electronic surveillance and physical search applications. In the area of foreign intelligence collection, the prescribed change was from "the purpose" to "a purpose."

- In explaining its rationale, President Bush's administration stated that such a change would "eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities which is critical to the success of anti-terrorism efforts."

- Associate Deputy Attorney General David Kris testified at a September 24, 2001, hearing on the legislation that "the animating purpose" of the change was to "bring those two sides together, allow for a single unified, cohesive response, and avoid splintering and fragmentation."

- Even then, some civil libertarians expressed concern. Critics of the legislation thought that simply requiring that foreign intelligence be "a purpose" of the collection was too big a blank check for the government to make use of FISA. As a compromise, the law was changed from "the purpose" to "a significant purpose." Buried in this change was a legal determination and also a cultural critique.

- Congress was calling for greater coordination and less concern about protective legal standards. So, as a legal matter, that is where matters fell after 9/11.

- The FISA Court of Review, as an appeals court for the FISA Court itself, summarized the new standard. It said that the FISA Court should not

deny an application if "ordinary crimes" were "inextricably intertwined with foreign intelligence crimes."

- For example, a terrorist who commits bank robberies to finance terrorist activity could be targeted using FISA's less-stringent standards. As long as foreign intelligence was a "realistic option," using the relaxed FISA procedures was acceptable.

- On the other hand, the review court said that the "FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes." As a result, to meet the new "significant purpose" test, the government need only "articulate a broader objective than criminal prosecution when applying to the FISA Court for authority to conduct surveillance. Such broader objectives could include stopping an ongoing conspiracy."

Questions to Consider

1. Which is more important in controlling government: law or culture? Why?
2. We often overreact to crisis. Did America overreact to the Church Commission? To September 11th? To both? To neither?

The U.S. Spy Network in Action

The big intelligence organizations that you are probably familiar with—the CIA and the NSA—are only two of at least 17 standalone offices of what we call the Intelligence Community. The goal of this lecture is to help you get a sense of the breadth of the intelligence enterprise: how it is structured, how it functions, how it relates to the rest of government, and maybe even why it is the way it is.

The Intelligence Community

- The Intelligence Community (IC) today is very different from what it was just a few years ago. In the immediate aftermath of the 9/11 terror attacks, the nation's government leaders concluded that our intelligence apparatus had failed us. So, we made an effort to fix it.

- Prior to 9/11, the many intelligence agencies (and there were fewer back then) were quasi-independent fiefdoms. The head of the CIA actually had two jobs: He ran the agency, and he was the Director of Central Intelligence (DCI) with nominal coordinating functions over all of the other intelligence agencies.

- This arrangement might have made sense early on, when the CIA was the preeminent agency in the IC, but in later years, it proved to be very challenging. For one thing, it is difficult for any one person to do two jobs. For another, the DCI had very little authority over other components of the IC.

- When Congress took a close look at this after 9/11, they didn't like what they saw. The Intelligence Reform and Terrorism Prevention Act of 2004 established the Office of the Director of National Intelligence (ODNI). The idea was that a single coordinating structure would unify the IC and manage its efforts.

- The ODNI will tell you that the resulting structure is more or less a federation intended to maximize the effectiveness of intelligence collection and dissemination among 17 member agencies while maintaining independence of action among each. Thus, the director's "role is to organize and coordinate" the efforts of the various agencies "to meet previously determined intelligence needs."

- One important limitation is worth noting. The office's budgetary authority is limited to the civilian side—the National Intelligence Program. As part of the back and forth that led to the creation of the office, the Department of Defense carved out the Military Intelligence Program, which is controlled by the Under Secretary of Defense for Intelligence. In practice, this means that large swaths of the IC—including the Defense Intelligence Agency and the NSA— are not formally within the control of the Director of National Intelligence.

- Another innovation of the 2004 law was to establish several national hubs responsible for developing collaborative approaches to the collection and analysis of intelligence for a specific issue.

- The National Counterterrorism Center (NCTC) doesn't actually collect any information on its own account, but it is designed to serve as the central repository for making connections between all available pieces of information about terrorism that the IC collects. Except for purely domestic terrorism, all of the data that we collect on potential terrorist threats goes through this hub.

- The Office of the National Counterintelligence Executive (ONCIX) is a horse of a different color. Counterintelligence is the art of trying to find the other side's spies, and the job of finding internal spies is managed by this central executive organization.

What Does the Intelligence Community Do, and How Does It Do It?

- The job of the IC is to collect and analyze information, creating intelligence. The people in the IC will tell you that creating good

intelligence is a multistage process—from requirements, to collection, to processing, to analysis, to dissemination.

- Consider the Russian leader Vladimir Putin and what he might have been intending to do in the Ukraine prior to the Russian-backed uprising in the eastern part of the country. Here's how the IC would approach the problem.

- First, the IC has to set priorities and define what target they are interested in. The Director of National Intelligence—in consultation with the director of the CIA and the director of the NSA—would identify Putin's Ukrainian intentions as a significant strategic issue. In doing so, they would be responding to consultations they also held with the Department of Defense, the Department of State, and the president's advisors at the National Security Council.

- Through that collaborative process, the need to understand what was in Putin's mind would become identified. Through a similar process, they might also decide that they needed to know North Korea's intentions for its nuclear weapons.

- Once a requirement is identified, the IC will begin to plan an information-gathering campaign to answer the requirement. Some collection might happen through human intelligence (called HUMINT). Some might happen through signals intelligence (called SIGINT), which is the interception of communications. And some might be acquired through image intelligence (IMGINT), such as satellite photographs of Russian troop movements.

- The National Geospatial-Intelligence Agency (NGA) is one of the newest intelligence operations, with its own acronym, GEOINT. Established in 1996 (under the name National Imagery and Mapping Agency), the NGA charts 116 million square miles of ocean and keeps electronic files on 45,000 airfields worldwide. It integrates that information with other intelligence to reveal where threats might arise, what their patterns of activity are, and how those forces relate to other pieces of the picture.

- Let's keep thinking about Putin in the Ukraine and examine who the NGA might help. But instead of using classified sources, let's consider what can be done using open-source satellite imagery.

- After the breakaway effort in eastern Ukraine got underway—and even as Russian authorities disclaimed any direct involvement—a research institution in Washington called the Atlantic Council released an analysis based, in part, on the freely available Internet-based services Google Earth and YouTube. They found photographs of large craters in Ukraine and videos of rocket launchers on nearby Russian territory, and they figured out that Russian units had fired across the border.

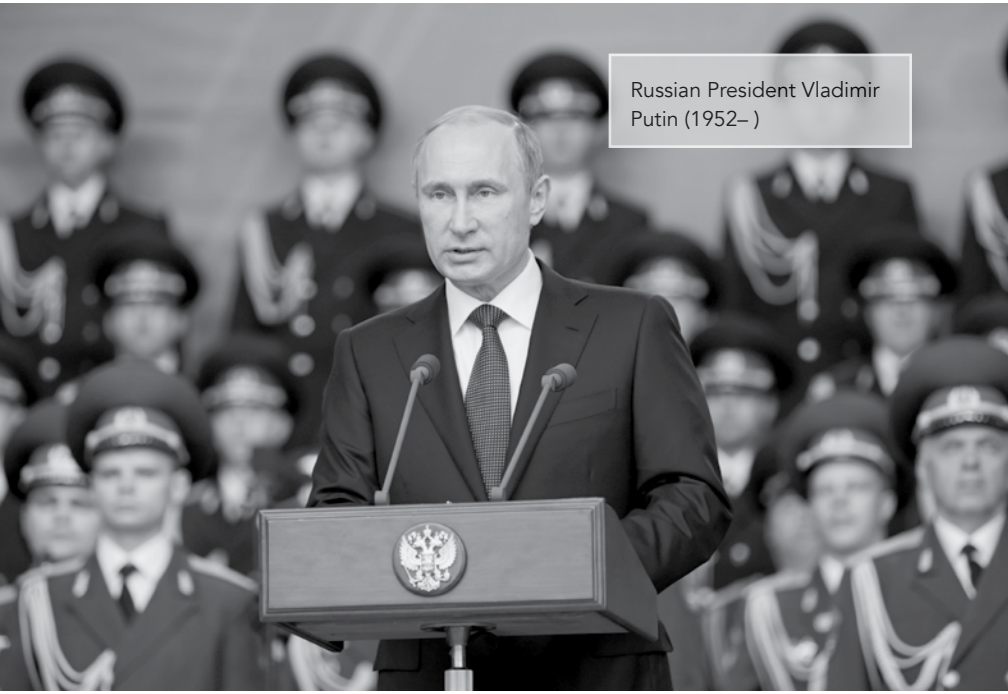
- The report also used satellite photographs (along with indiscreet social media posts by Russian soldiers) to identify the Russian military camps being built near the border. Tracking by satellites photographs, video, and other visual evidence also enabled the Atlantic Council to track what it identified as Russian rocket launchers, tanks, and so on. The bottom line was pretty clear: Russian troops and gear were operating in Ukraine territory.

- And if we can reach that conclusion readily using publicly available information, the NGA likely had even more convincing data.

- The information collected doesn't necessarily come in pristine form. Some images, for example, need to be processed through image-enhancing technology. Encrypted communications need to be decrypted, and the codes that protect them need to be broken. Even human intelligence needs to be interpreted, or processed in some sense, to the extent that we are constantly evaluating the credibility of our spies and their capabilities.

- Eventually, the IC gathers all the information that it reasonably—or not so reasonably—can about a particular topic.

- Then comes possibly the most important phase of the intelligence-production cycle: analysis. What exactly do Russian troop movements



Russian President Vladimir Putin (1952–)

on the Ukrainian border portend? What does our image intelligence show us? Does it match or conflict with what we think we know from the interception of Russian communications? And how does all of this fit into the overarching economic circumstances that Russia finds itself in because of, for example, the price of oil?

- One thing that is often lost on people outside of the IC is how dependent intelligence analysis is on the concatenation of small, seemingly disparate pieces of information. Sound analysis is often derived from deductive reasoning. In the end, the process might produce some findings and a scenario forecast accompanied by a statement of the degree of confidence with which the analyst views his or her findings and forecast.

- Satellite imagery of Russian troops moving to the border might be combined with economic analysis of Russia's oil reserves and human intelligence from someone who recently participated in a discussion with Vladimir Putin.

- On important matters such as this, the IC would collect all the information available to it, and it would use a number of analysts to produce a National Intelligence Estimate reflecting the considered judgment of the community. Such judgments are not always correct, of course, but we can't expect perfection in analyses of human behavior.

- Finally, there is the issue of dissemination. Sharing the assembled data and analysis tends to compromise the sources and methods by which the information was initially collected. It also gives those who read the analysis an insight into the analytic strengths and weaknesses of the authoring agency. Distribution of this sort of information is usually limited to a select few—ideally, those who will best benefit from it.

How Big Is the Intelligence Enterprise of the U.S. Government?

- *The Washington Post* reviewed thousands of documents and interviewed scores of people to compile the first unclassified database of American intelligence activity in a report a few years ago that it headlined as "Top Secret America."

- *The Post* identified 1,271 government organizations and 1,931 private companies as part of the IC. They were in roughly 10,000 locations in the United States and were working on counterterrorism, homeland security, and intelligence. *The Post* also reported that at least 854,000 people working in the IC held top-secret clearances.

- The U.S. intelligence budget (excluding the Military Intelligence Program) is currently in the range of 50 billion dollars and rose by about one-third during the more than decade-long War on Terror.

- Of course, the budget disclosure is deficient in a few ways: It doesn't include the military portion of our intelligence system (which is quite

large), and it is just the "top line" of the budget. In other words, we don't know how the money is divided among the 17 intelligence agencies.

Questions to Consider

1. The intelligence community is such a sprawling enterprise. How can it best be controlled by elected officials?
2. Who should decide what gets classified? What is the basis for making that decision?

Big Data's Shadow

Every click you take in cyberspace can be tracked, your cell phone broadcasts your geolocation, and all of your purchases and phone calls are cataloged somewhere. Taken together, this information can be analyzed to paint a picture of you—one that, increasingly, others can see. It might define who you are and let users predict what you will do in the future. The result is a loss of privacy. After all, the problem with such data—so-called big data—is the magnification of its effect by how pervasive it is.

Big Data

- In an increasingly networked world, personal information is widely collected and widely available. As the storehouse of personal data has grown, so have governmental and commercial efforts to use this data for their own purposes.

- Commercial enterprises solicit new customers with targeted ads. Governments use the data to identify and locate previously unknown terror suspects—so-called clean skins, who are not in any intelligence database. We have discovered that we can link together individual bits of data to build a picture of a person that is more detailed than the individual parts.

- Big data offers all kinds of opportunities to those who have access to it. But this also comes at a price: It creates an ineradicable trove of information about us as individuals, making it increasingly difficult to safeguard our privacy.

- If the government collects data to build a picture of, for example, a previously undetected terrorist threat, it can also—if it is so minded—use this capability to build a picture of its political opponents. That navigable web of data poses threats in the Free World and, perhaps even more so, in authoritarian nations.

Your cell phone broadcasts your geolocation, and all of your purchases and phone calls are cataloged.

- In thinking about this capability and the opportunities and threats it presents, we sometimes talk out of both sides of our mouths.

- Early in the century, there was significant hype surrounding the government's launch of one such big data program, known as Total Information Awareness. It was a research project of the Defense Advanced Research Projects Agency (DARPA) in the immediate aftermath of the 9/11 terror attacks.

- DARPA's working premise was that advanced data-analysis techniques could be used to search the information space of commercial and public-sector data and identify threat signatures indicative of a terrorist threat. Because this would have given the government access to vast

quantities of data about individuals, it was decried as the harbinger of Big Brother and was eventually killed.

- Compare that public condemnation and the government's reflexive response with the subsequent, almost universal criticism of the intelligence sector's inability to connect the dots prior to a subsequent terrorist plot. This was the plan of the young Nigerian Umar Farouk Abdulmutallab to detonate an explosive aboard a jumbo jetliner, on an international flight bound for the United States on Christmas Day in 2009. Also known as the "underwear bomber," he subsequently was sentenced in a U.S. court to life in prison.

- In that instance, we were told that we did not perform enough data analysis. We failed to link National Security Agency intercepts to airline travel records and State Department reports.

- The conundrum arises because the analytical techniques of big data are fundamentally similar to those used by traditional law-enforcement agencies. We use analytic algorithms to take a lead (a single piece of information as a starting point) and follow it to identify connections.

- This is what the police do on a daily basis, but in the big data system, computer systems operate on a much more vast set of data. And that data is much more readily subject to analysis and manipulation. As a result, the differences in degree between what the police used to do and what computer analysis can do today tend to become differences in kind.

- The ability to collect and analyze vast quantities of data is a fundamental change caused by technological advances that cannot be stopped or slowed. The phenomenon derives from two related yet distinct trends: increases in computing power and decreases in data storage costs.

Big Databases

- In the late 1980s—practically the dawn of time for personal computers—the Department of Justice went to a great deal of trouble to create a database with information about the criminal records of known

offenders. These records were kept in disparate local, state, and federal databases.

- All of these records were generally public and, in theory, available for inspection by the media and private citizens. But in practice, the information was so widely scattered that no crusading journalist or enterprising individual could incur the expense of finding it all and creating a comprehensive dossier on any individual.

- Only the federal government possessed the degree of need and adequacy of resources to undertake the task of creating the precursor of what is today the National Crime Information Center. At very great expense, the Department of Justice began to collect criminal records on a small number of criminals who were of national interest.

- Then, large data-collection and data-aggregation companies, such as Experian and ChoicePoint, began to harvest—by hand—public records from government databases. These data-aggregation companies systematically compile birth records, credit and conviction records, real estate transactions and liens, bridal registries, and even kennel club records. One company, Acxiom, estimates that it holds, on average, approximately 1,500 pieces of data on each adult American.

- Anyone with enough data and sufficient computing power can develop a detailed picture of virtually any identifiable individual.

Big Data Failure

- Two of the 9/11 terrorists made reservations on American Airlines Flight 77. Their names also happened to be on the CIA's watch list. But we didn't connect those two pieces of information. If we had, we could have identified their home addresses from information they provided to the airline.

- And a simple cross-check would have discovered that three other individuals associated with these addresses—one of them named Mohammed Atta—also had made flight reservations on September 11th.

- If we cross-checked the callback phone number that Atta gave to the airline, we'd likely have discovered that five other individuals also had provided that same phone number to reservation agents for purposes of confirming their own flight reservations on September 11th.

- And had we looked in one more place in the airline database, we would have discovered the name of yet one more individual who used the same frequent flyer number as had one of the men on the CIA watch list. Then, if we had branched out to public sources, we would have found that two more individuals shared living arrangements—that is, they had the same address.

- Finally, the remaining six individuals associated with hijacking four commercial airplanes on that date—and launching them into the World Trade Center in New York and into the Pentagon in Washington DC, as well as the lone misfire that went astray on an empty field in Pennsylvania—could have been identified through a routine review of U.S. Immigration and Naturalization Service's records (the expired visa/illegal entry list). One terrorist was on that list, and five others had public records of having lived with him or among each other.

- And all, of course, shared the common characteristic of making reservations on flights for the morning of September 11th. In short, as a Department of Defense review committee concluded, with just seven clicks of the mouse through existing databases, all 19 terrorists could have been identified and linked to one another.

Big Data Success

- Ra'ed al-Banna—a Jordanian who attempted to enter the United States via Chicago on June 14, 2003—was probably a clean skin (a terrorist with no known record). He was carrying a valid business visa in his Jordanian passport and outwardly appeared to be an unremarkable business traveler from the Middle East.

- The Department of Homeland Security operates a sophisticated data-analysis program called the Automated Targeting System (ATS) to assess

The aftermath of the September 11, 2001 terrorist attacks in New York City

the comparative risks of arriving passengers. Homeland Security uses ATS to decide who to stop and talk to and who to let through easily. The system has become essential, given the sheer volume of travelers to the United States.

- ATS flagged al-Banna for heightened scrutiny. He was pulled from the main line of entrants at Chicago's O'Hare Airport and was individually questioned.

- During the interview, al-Banna's answers were inconsistent and evasive—so much so that the U.S. Customs and Border Protection officer who conducted the interview decided to deny his application for entry and ordered him returned to his point of origin. As a matter of routine, al-

Banna's photograph and fingerprints were collected before he was sent on his way.

- The story might have ended there, because Customs and Border Protection officers reject entry applications daily for a host of reasons. But al-Banna proved to be an unusual case.

- More than a year later, in February 2005, a car filled with explosives rolled into a crowd of military and police recruits in the town of Hillah, Iraq. More than 125 people died—the largest death toll for a single incident in Iraq until that time.

- The suicide bomber's hand and forearm were found chained to the steering wheel of the exploded car. After U.S. forces took fingerprints, a match was found to al-Banna's in Chicago 20 months earlier.

Questions to Consider

1. It is shocking and disturbing that the government had information in hand that might have been used to prevent 9/11. How can we avoid that problem in the future without giving too much information to the government?
2. Do you use E-ZPass, or a similar automatic toll-paying device? Do you worry about the data being collected? If not, why not? If you do, why?

Some Problems with Privacy

Our current privacy rules are simply not up to the task of anticipating and accommodating every demand for interpretation and application presented to them in the privacy debate. They are, to a very real degree, relics of the last century. Many of the relevant federal statutes and Supreme Court precedents date from the 1970s. So, rather than focus on law, this lecture will discuss privacy as a defined set of practices and processes.

Concepts of Privacy

- Our concepts of privacy today are largely embedded in a set of principles known as the Fair Information Practice Principles (FIPPs), which the United States developed in the early 1970s and which are the keystone of the Privacy Act of 1974.

- The principles state that a government should limit the collection of personal information to what is necessary, use it only for specific and limited purposes, be transparent and open with the public about how the information is collected and used, and allow the individual about whom the data is collected to see the data and correct it if necessary.

- New technologies, such as drones, biometrics, and big data collection and analysis destroy these types of rules. A conscientious and fair application of such principles is, in many ways, fundamentally inconsistent with the way in which personal information is used in the context of counterterrorism or, for that matter, in commercial data analysis.

- Consider, for example, the purpose and use-specification principle, which states that data collected for one purpose should not be used for another. If universally applied, this principle would make it impossible for many sophisticated knowledge-discovery systems based on big data analysis to work well. Often, the data that provides us with the necessary missing link—from law enforcement to scientific research—is

information that was collected for a different purpose and intended for a different use.

- In a world of widely distributed networks—with massive data storage capacity and computational capacity—so much analysis becomes possible that the old principles no longer fit. What is needed, then, is a modern conception of privacy: one with enough flexibility to allow effective government action but with the surety necessary to protect against governmental abuse.

- Some people think that the old privacy rules should be reinforced. But technology is forcing change. The old ideas of collection and purpose limitations are obsolete and need to be replaced because they can't withstand the onslaught of new privacy-invading technology that all, or most, people embrace.

- Instead, we should focus on how data is used. And, more importantly, we should recalibrate our laws so that our concern is not with uses that are mere "analyses," but rather with uses that constitute the "imposition of adverse consequences." The focus should turn to actual harm to an individual: If the analysis, for example, wrongly puts a person on a no-fly list or denies the person a job, that would be the sort of adverse consequence we would strive to avoid.

- There are a few building blocks for this idea. First, we really need to dig deep into what we mean by privacy. Privacy is a misnomer in some respects. What it reflects is a desire for the independence of personal activity—a form of autonomy.

- We protect that privacy in many ways. Sometimes, we do so through secrecy, which effectively obscures the observation of conduct and the identity of those engaging in the conduct. In other instances, we protect your autonomy directly by allowing you to exercise your own individual choice of conduct. Indeed, the whole point of that kind of privacy is to allow people to act as they wish in public, which is a different way of looking at privacy.

- Anonymity is a third concept of privacy, the one that is most relevant to our consideration of the changes brought about by new technology. It's a kind of middle ground where observation is permitted—that is, we expose our actions in public—but where our identities and intentions are not ordinarily subject to close scrutiny.

- In everyday life, we leave behind an electronic data trail that is suffused with information of this middle ground sort, including bank account transactions, phone records, airplane reservations, and smart card travel logs.

- Likewise, the physical realm of biometrics and drones often involves the collection of publicly exposed information in which we have an anonymity-based privacy interest. These forms of information—partially public, but with an overlay of privacy—constitute the core of the transactions and information available to governments.

- The type of anonymity that one has in respect to our activities in the electronic realm or under the gaze of unseen drones is not terribly different from the type of anonymity we have every day in our physical existence.

- Protecting the anonymity we value requires, in the first instance, defining it accurately. One might posit that anonymity is, in effect, the ability to walk through the world unexamined. That is, however, not strictly accurate, because our conduct is examined numerous times each day.

- Sometimes, the examination is by a private individual, such as an individual sitting next to you on a train. Other routine examinations are by governmental authorities and commercial entities, such as the policeman who watches the street and the security camera that records people at the bank.

- So, what we really must mean by anonymity is not a pure form of privacy akin to secrecy. Rather, what we mean is that even though one's conduct is examined routinely and regularly—both with and without one's knowledge—nothing adverse should happen to you without good cause. In other words, the veil of anonymity is now readily pierced by technology.

- So, to actively protect privacy that otherwise is compromised by the new technology, we must formulate rules that prescribe limits to such unwanted and undesirable intrusions. These rules are needed to protect our privacy and prevent governmental abuse.

- The key to this conception is that privacy's principal virtue is a limitation on consequence. In the context of governmental oversight, the questions to be asked of any new surveillance program are as follows: What is the consequence of identification? What is the trigger for that consequence? Who decides when the trigger is met?

Protecting Privacy

- The traditional way to protect privacy, as well as its essential component of anonymity, is with a system of rules and a system of oversight for

compliance with those rules. Here, too, modifications need to be made in light of technological change.

- We have begun to develop new systems and structures to replace the old privacy systems. First, we are changing the way we protect privacy from a top-down process of rules to one in which the principal means of privacy protection is through institutional oversight.

- Such institutions as the Department of Homeland Security, the 2004 Intelligence Reform and Terrorism Prevention Act, and the independent Privacy and Civil Liberties Oversight Board are, in effect, internal watchdogs for privacy concerns. In addition, they naturally serve as a focus for external complaints, requiring them to exercise some of the functions of ombudsmen. In either capacity, they are in a position to influence and change how the government approaches the privacy of its citizens.

- Perhaps most significantly, the same surveillance systems our government uses to advance its interests are equally well suited to ensure that government officials comply with the limitations imposed on them in respect of individual privacy. Some surveillance systems can be uniquely well equipped to watch the watchers, and there are already indications that strong audit mechanisms, when in place, can be effective.

- If we did reconfigure our conception of privacy, put the right control systems in place, and use a strong audit system for the government, we could be reasonably confident that a consequence-based system of privacy protection would move us toward a place where real legal protections could be maintained.

- It wouldn't be perfect; there would always be mistakes and abuses. And it would be much more difficult to manage in the real world than the pure privacy protections we have in place now. But we need a solution that is more in sync with today's technological realities, and these ideas should at least get us a little closer.

Privacy in the Commercial Sector

- In the commercial sector, we see a whole different set of challenges. To begin, the Constitution doesn't apply to private commercial actors, so that's not a potential avenue for protecting privacy.

- On the other hand, the field is wide open for Congress to regulate. Unlike government surveillance—where the purpose is, at least theoretically, to protect national security—when Congress steps in to limit commercial surveillance, the only negative consequence might be to interfere in the development of new technologies and markets.

- At this point, the value of commercial use of new technology has become so deeply embedded in the business model of corporate America that it will be difficult to modify. Commercial companies value the information they gather about you. It lets them know what to sell you or how to try to influence you.

- Some web services are free precisely because the accumulation of your data is their product. If we change that business model—and we can—then, in the end, you will have to pay for some web-based services that currently have no direct cost to you.

- However, in the commercial sphere, we are already moving toward a system that looks more like the "consequence" idea of privacy. In order to protect your privacy and prevent the misuse of your data, you need to know what will happen to it, and you need to be able to control the use of it. Slowly, the laws are moving that way.

- Increasingly, companies are being criticized for overly invasive uses of your data, and they are changing what they do. Throughout the world, but especially in Europe, free web services are being called to account and told to publicize what they do (and to build in options that allow you to manage how your data is collected and used). The commercial sector is resisting, but the trend is pretty clear.

Transparency

- A flip side to the loss of privacy is a gain in transparency. This can be valuable to the extent that it gives citizens insight into the actions of their governments. And just as citizens find that they are losing their privacy, we are quickly coming to the point where governments won't be able to keep secrets very well, either.

- The development of technology has made it very difficult, for example, for an undercover spy to move around with a false identity. While some governments might think that's a problem, some people might believe it's a good thing.

- Privacy and transparency are two sides of one coin, and we associate very different values with each of them, depending on how they are applied and to what end. We neither want to live in a world of one-way surveillance, nor do we wish to live in a world where some can live invisibly. Privacy requires a balance.

Questions to Consider

1. If you had to choose, which would you prefer for your life: the Ring of Gyges or the Panopticon?
2. You don't have to choose, obviously, so how do you decide when privacy should prevail and when transparency should? And who gets to make that choice?

Under Observation: The Panopticon Effect

British philosopher Jeremy Bentham proposed erecting a hotel, or a jail, in circular form—with a watchman at the center and the resident guests on the periphery. In this way, one person could keep a careful eye on everyone else. Bentham called this building the Panopticon, and the reaction of those under observation came to be known as the Panopticon effect. In this lecture, you'll learn about the effects—both positive and negative—that observation has on our conduct. You'll also learn about the effects of social behavior when it is anonymous. Furthermore, you'll learn about the effects that observation has on the watchman.

Observation and Human Behavior

- Most Western governments don't take prurient interest in their citizens' private lives, and a wide range of safeguards normally is erected to maintain this healthy barrier. But social science tells us that harm can happen even when the government is not actively looking over our shoulders. There is a self-editing effect that arises from the perception of scrutiny.

- There might not be a great deal of self-editing among many people, but sometimes those who lead lives on the edges of social convention—politically, culturally, or behaviorally—might edit their behavior out of a concern for how their actions will be perceived.

- But the observer effect is as real in social structures as it is in physics. That's why schools have proctors in exam rooms. The very specter of surveillance and its effects on behavior can be characterized by some as a cognizable harm to their liberty.

- In the 1950s—at the height of anti-Communist feelings during the Cold War—government employees and professors in Washington DC came under closer scrutiny. As a result, many of them withdrew from

nongovernmental organizations, cancelled subscriptions, declined to participate in petition drives, and became more cautious in their conversations with strangers. This reflects, on a smaller scale, the same reaction to surveillance as seen in other nations where surveillance is overt and pervasive.

- But the observer effect is more widespread than what arises from gross and intrusive surveillance. One study by the Australian academic Shane Dawson, who specializes in social network analysis, looked at how institutional surveillance technologies affected student behavior in educational environments. Dawson found that the students' Internet-browsing behaviors, as well as the range of topics they discussed in online forums and the writing styles they employed, were influenced by the degree to which they understood their activities to be under surveillance by the educational institution.

- It is worth noting that the adverse effects of observation are not limited to government surveillance. In our evermore-transparent society, which is galvanized by the proliferation of social media, the malign effects of public observation are often on display, most notably through acts of public shaming.

- The British journalist Jon Ronson cataloged some aberrant instances in his book, *So You've Been Publicly Shamed*. He tells the story, for example, of Justine Sacco, a New Yorker who tweeted an offensive joke to her followers just before boarding a long flight to South Africa. Her tweet was retweeted and went viral. She lost her job and suffered months of online harassment—probably much harsher punishment than one very poorly thought-out tweet deserved.

- Alice Marwick, a postdoctoral researcher in social media at Microsoft, calls this type of public monitoring "social surveillance." She has documented how it has behavioral-modification effects on teenagers who have profiles on social networks. Because of the observer effect, these teens consciously shape their external image and modify their online behavior—mostly to satisfy the social pressure of other teens.

Some conformity is the inevitable result. We also see more surreptitious social surveillance (Facebook stalking).

- Our instinct to observe and judge others is a dark side of the Panopticon, no matter who wields the watchers' spectacles. These public shamings, distributed via social media, are commentaries that we hope never to read about ourselves. But, certainly, everyone has something to hide.

- The watchman's observing eye can also, of course, have positive effects. One notable place we have seen this phenomenon is in the actions of corporations subject to public scrutiny under the law. So-called right-to-know laws often mandate that companies disclose sensitive details about their operations—how much of a pollutant, for example, they discharge into a local river. These laws have had the salutary effect of driving pollution reduction without mandates.

- This demonstrates that public observation—a form of mass surveillance—can have a positive effect on societally undesirable behavior. The same goes for government surveillance of the citizenry. Sometimes, governments can produce social benefits with surveillance and data collection.

- In 2014, Ebola raged in Western Africa. Doctors fought to stem the flood, aided by big data. They used mobile phones owned by West Africans that were equipped with geolocation capabilities—that is, the ability to broadcast the unit's geographic location. Using voice and text data, the authorities tracked population movements in the region and figured out the best places to set up treatment centers. They also identified which areas to quarantine.

Anonymity and Human Behavior

- Some evidence suggests that, in the absence of a watchful eye, anonymity fosters aberrantly bad behavior. But in other ways, anonymity allows for positive social engagement.

The anonymity that the Internet offers causes some people to say and do things they might not say or do if others knew their identity.

- We commonly recognize that anonymous actors are ruder and more abusive than those we can identify. The most common place we see this is in the cyber domain, where anonymity is common. This is sometimes known as the online disinhibition effect. Social norms that are present in face-to-face conversations seem to disappear in the cyber world.

- We aren't sure exactly where this lack of inhibition comes from. To be sure, some of it arises from anonymity.

- Some also stems from the related, yet distinct, problem of invisibility: If you can't see me, then you can't read the social clues I'm sending, and if I can't see you, then I can't know who you are, so I can't relate to you.

- A third cause is sometimes called asynchronicity: We aren't talking to each other in the same place at the same time, which makes it easy to leave a message that is volatile and inflammatory, and then just disappear.

- Still other sources of the lack of inhibition might be the idea of fantasy; many conversations seem less real when they take place in the cyber domain. Some people see it as a second world, where life is just a game, and the regular rules of conduct (i.e., obligations to honesty or kindness) don't apply.

- The sad rise of cyberbullying is a particularly unfortunate example of such harmful behavior. Even though the conduct is increasingly subject to criminalization, it continues. Anonymity makes it more difficult to identify bad actors, so they continue to act badly.

- Professors Keith Wilcox of Columbia University and Andrew T. Stephen of the University of Pittsburgh found that in social networks that allow for anonymity—as in the use of pseudonymous screen names—people tend to present a positive self-view of themselves to others. This leads to increases in self-esteem, albeit while also tending to reduce self-control.

- This is a different way of looking at the same anonymity issue. The conclusion of Wilcox and Stephen is pretty positive. In their view, people post comments on Facebook that they would probably never say aloud—not because they are mean, but because they feel empowered.

Psychological Effects of Observers

- There are psychological effects that arise specifically from being in a position to watch. In the movie *The Lives of Others*, about East Germany's Stasi system of state surveillance, a crucial transformation takes place in the psyche of the watcher, Gerd Weisler. At the start of

the movie, he is a loyal party spy. By the end, the intrusiveness of his own watching and listening has changed him so much that he betrays the state Communist party.

- Although one might hope to imagine that the psychological effect of being a watcher is always so salutary, sadly we know that isn't the case. Among the best recent evidence for the bleak downside is the stress registered by some surveillance drone operators, whom we can think of as contemporary, technology-empowered observers.

- For years, psychologists thought that post-traumatic stress disorder (PTSD) arose from "fear conditioning"—that is, from the lasting psychological ramifications of mortal terror. Drone pilots typically don't experience that fear. They are physically safe, far away from the battlefield.

- But some suffer from PTSD, nevertheless—not because of any physical violence inflicted on them but, rather, due to their sensitivity to the violence they witness inflicted on others, or perhaps even reflecting the watchman's failure, or inability, to do anything about it.

- Not all observers suffer equally. Many, it seems, are readily able to disassociate themselves from what they are seeing and doing. Somehow, for example, many of the guards at Nazi concentration camps during World War II were able to internalize the horrific depredations they administered.

- The lead Nazi exterminator, Adolph Eichmann, and others like him, expressed no outward effect from observing and orchestrating the greatest atrocities. It is a result that most people find extremely puzzling and very disturbing.

- As with most issues of psychology, the overall sum of evidence is somewhat inconclusive. But it is fair to say that the evidence confirms our instincts. We certainly see ways in which observation can enforce good behavior, but it also creates incentives for excess.

Questions to Consider

1. If you had taken the Milgram test, how would you have reacted?
2. Have you ever used an anonymizing feature on the web? Why? How do you react when someone else uses that feature and keeps their identity from you?

Drones, Drones Everywhere

Manufacturers call them unmanned aerial vehicles (UAVs)—or, more grandly, unmanned aircraft systems (UASs)—but the rest of the world calls them drones. As drone applications proliferate, rules on their use and boundaries that should apply remain unclear. In this lecture, you'll learn about drone technology so that you might better understand how drones works and what they are capable of. Then, you'll examine some domestic uses of drones. Furthermore, you'll consider some unique legal and policy issues, asking how we, as a society, are going to deal with this technology.

How Drones Work

- For most people, the word "drone" conjures up the image of a lethal, missile-armed Predator or Reaper, such as the drones deployed in the Iraq and Afghanistan wars and afterward. Once the United States demonstrated the Predator's capabilities, drones became an indispensable military tool—and part of our vocabulary. But military drones are a small fraction of the types of drones used in the United States and around the world today.

- The Israelis were the first to design the modern, glider-type drone in the 1970s. They built small, lightweight devices, making them inexpensive to build—and difficult to shoot down. Larger drones soon followed, and today some of them are quite large.

- Thousands of drone platforms now exist for a wide variety of purposes, from scientific research to military operations. Drones are employed by governments and by the private sector.

- Drones themselves are unmanned, but they are controlled by a human operator. These remote operators typically are highly skilled and must be trained for their particular missions.

Surveillance drone on patrol over New York City

- In the military, drone pilots learn how to carry out intelligence, surveillance, and reconnaissance missions and also how to conduct and respond to electronic attacks, implement strike missions with weapons, conduct search-and-rescue operations, and so on. For the military, remote piloting greatly reduces the risks to U.S. personnel and makes the vehicles cheaper to produce.

- The last point often gets overlooked. Although drones are unmanned, trained crews steer the craft, analyze the images that the cameras send back, and act on what they see. In the military context, that might mean firing missiles at a surveilled target. In a civilian context, it might mean taking photographs.

- Drones are not autonomous—at least not yet. A human is always in the loop. The control base for this remotely piloted vehicle can be anywhere that you are able to establish a communications link.

- The control system is the most intricate part of the system. Commands from the controller are encrypted and uplinked to satellite, which then downlinks the commands to the drone. Drone sensor data flows back along the same channel—or, if you want, the sensor data can be directly shared with others.

What Drones Do

- Drones are used in both military and domestic applications.

- In 2015, the Pentagon reportedly controlled about 7,000 military-grade drones—up from fewer than 50 at the start of the 21st century. These have been used increasingly in military missions overseas, first running reconnaissance and then targeting al-Qaeda operatives in Afghanistan, Iraq, Pakistan, Somalia, Yemen, and elsewhere.

- Meanwhile, such hostile groups as the Islamic State of Iraq and al-Sham (ISIS), Hamas, and Hezbollah are said to have obtained their own drones. The inevitable result of such proliferation is that malevolent uses could become a problem in the United States.

- The Department of Homeland Security uses drones for Border Patrol security. These vehicles conduct surveillance of areas and routes that are inaccessible to regular patrols. Likewise, we use drones over the ocean to maintain maritime domain awareness and to track shipping headed to the United States.

- We use drones for emergency preparation and disaster response. Before the next hurricane hits, drones will have planned evacuation routes and anticipated vulnerable locations. In the immediate aftermath of as major storm, they also allow us to observe the catastrophic effects and begin remediation planning. And drones can provide emergency restoration of cell phone coverage.

- By providing a visible police presence, drones deter criminal behavior in unpatrolled areas. United Nations peacekeepers are using drones for the same kinds of reasons.

- In agriculture, farmers use drones to monitor crop growth at a local level and in greater detail than might be provided, for example, by satellite photos. Drones have even been used as a replacement for crop-dusting airplanes as a way of spraying pesticides and eradicating pest infestation.

- Meanwhile, scientists and environmentalists are increasingly using drones for environmental monitoring, as well. With these aerial vehicles, we can track wildlife, monitor droughts (or flooding), and watch the stability of locks, dams, and levees in remote areas.

- With the right equipment, drones can sample the pollution over our cities and test concentrations of carbon dioxide concentration in remote locations. They might even fly into the eye of a hurricane without risking human life. Anywhere that humans can go or might want to go—to see or do something—is potentially a place where drones can lead us.

- One of the most interesting commercial applications is the use of drones by newsgathering operations. Drones are much cheaper to operate than traffic helicopters. And when large demonstrations occur, they can provide a safe platform for news gathering.

- Of course, drones are also going to be used by paparazzi to stalk celebrities. Film crews are another big user. Drones are cheaper and easier to use than helicopters. Big retailers and package-delivery services are interested in drones as distribution vehicles to reach consumers.

- Just as news organizations might want to employ drones to watch a riot as it unfolds (or some other event, for that matter), the government wants drones to enhance its law-enforcement and homeland security capabilities.

- We can readily imagine some government uses that would be appropriate—for example, for search-and-rescue missions. But still, because of their surveillance capabilities, drones could impinge on personal privacy and other civil liberties without proper legal guidelines and oversight.

- The proliferation of drones in our skies might also threaten aviation safety. We can prohibit certain uses altogether, of course. Using a drone to case a house for a burglary will still be a crime, just as burglary is now. And it is a near certainty that the Peeping Tom laws will be modified, if they need to be, to include a prohibition on drones.

- But hard questions will come from mixed uses—instances where data collection includes collateral collection of information and imagery. Market predictions suggest that the manufacture and sale of drones will be a multibillion-dollar industry. Whether we like it or not, drones are here to stay. Given their utility, it seems far more likely that we will control drone use through rules and regulations rather than ban them.

- First, there will be safety regulations. When first presented with the question, an administrative law judge said that absent written rules, the Federal Aviation Administration (FAA) couldn't regulate drones, because the court viewed them as being no different than model aircraft.

- That led the FAA to issue its first commercial drone license in June 2014, to BP (the former British Petroleum), which had requested permission to use a 13-pound drone to survey its equipment and pipelines in Prudhoe Bay, Alaska.

- At the same time it issued that first license, the FAA moved to restrict everyone else who didn't have one. Later, the FAA issued a draft of its proposed rules for hobbyists. They proposed that we can freely fly our small remote-controlled drones (weighing less than 50 pounds) as long as the drones stay away from airports, keep below 400 feet, and remain within the controller's sight.

- Anyone else, including news organizations, package-express companies, and retailers would have to wait for new regulations or get a one-off exemption. Few exemptions were issued initially (mostly for closed movie sets).

- It's possible that a final rule would require the operators of large drones to obtain air-worthiness certificates and fly them with licensed pilots. These requirements would be quite expensive. In the meantime, the current general prohibition stands.

Legal and Policy Issues

- Privacy and civil liberties issues pose still more interesting questions. On one side are some academic researchers who have been following the FAA debate. They contend that the FAA-imposed restrictions on drones would jeopardize their work and undermine basic education.

- On the other side of the coin is the state of California. California's legislature adopted a law requiring police departments throughout the state to get a warrant from a judge in almost every situation where they might use a drone, except for emergencies such as a hostage taking.

- Imagine that while on patrol for counterterrorist purposes, a drone spots images that might convey a drug deal. Or they could just be pictures of two guys meeting in the woods. Should the analysts who collect this data share it with the local police department?

- On one hand, the answer seems to be clearly yes. We don't want government officials to turn a blind eye during the course of their duties to a crime they happen upon. The Fourth Amendment, which prohibits unreasonable searches and seizures, likely would be no legal barrier to sharing the information.

- On the other hand, there's a good argument for the answer to be no. One way in which we limit government activities that impinge on civil liberties is through use limitations—that is, the idea that information

and data collected for a specific use can be used only for the particular purpose.

- One idea is to pass a law that would authorize data collected for counterterrorism purposes to be shared with police for other purposes only if those purposes involved "responding to, or otherwise preventing or mitigating, an imminent threat of death or serious bodily harm."

- The following are some other limitations that we might consider for drones.
  - The use of drones in a military capacity would be severely restricted to situations of actual invasion or insurrection.
  - The use of drones for domestic surveillance of First Amendment activity would be considered fundamentally at odds with U.S. constitutional principles and be prohibited.
  - Drones equipped with novel sensor arrays would not be permitted, absent a clearly demonstrated need and a careful consideration of countervailing privacy and civil liberties concerns.
  - Drones would not be used as a platform for the collection of massive unstructured data sets because that type of collection could form the basis for sophisticated tracking and behavioral analytics.
  - Drones would be considered unsuitable for use as a routine means of surveillance in nonthreatening situations.

- For all of these ideas, value judgments and choices need to be made. So, Congress has to be engaged. Technology and the law need to be harmonized to ensure that the state remains secure and its people remain free.

Questions to Consider

1. Are drones different from helicopters? Why, or why not?
2. Should you be allowed to stop a drone from flying over your house?
3. Would you want a drone delivering pizza to you?

Biometrics: Eyes, Fingers, Everything

In a post-9/11 world, we want to link the biographic information we have available to us about risks associated with an individual to a verifiable biometric characteristic—that is, a physical characteristic that is impossible to change. As a basic building block of risk assessment, we think it is imperative that we can have confidence that people are who they say they are. In this lecture, you'll discover what biometrics is, how it works, and what makes it useful. You'll also consider how the technology might threaten civil liberties.

Biometrics

- Biometrics is among the oldest of new technologies. It began with fingerprints early in the 20th century and today includes more novel ideas, such as gait recognition, which is the ability to identify an individual by his or her physical gait, or movement—that is, by how he or she walks.

- Biometrics can be used in two ways: for verification or for identification. When a biometric device is used to verify whether a person is whom he or she claims to be, that verification is frequently referred to as "one-to-one" matching. Almost all systems can determine whether there is a match between the person's presented biometric and biometric templates in a database in less than one second.

- Identification, by contrast, is known as "one-to-many" matching. In the one-to-many matching framework, a person's biometric signature—whether an iris or a fingerprint—is compared with all of the biometric templates within a database.

- There are two types of identification systems for this framework: positive and negative. Positive systems expect there to be a match between the biometric presented and the template. These systems are designed to make sure that a person is in the database. Negative systems are set up

to make sure that a person is not in the system. Negative identification can also take the form of a watch list, where a match triggers a notice to the appropriate authority for action.

- Neither system generates perfect matches (or exclusionary filters). Instead, each comparison generates a score of how close the presented biometric is to the stored template. The systems compare the score with a predefined number or with algorithms to determine whether the presented biometric and template are sufficiently close to be considered a match.

- Most biometric systems require an enrollment process, in which a sample biometric is captured, extracted, and encoded as a biometric template. This template is then stored in a database against which future comparisons will be made.

- When the biometric is used for verification (for example, access control), the biometric system confirms the validity of the claimed identity. When used for identification, the biometric technology compares a specific person's biometric with all of the stored biometric records to see if there is a match. For biometric technology to be effective, the database must be accurate and reasonably comprehensive.

Forms of Biometrics

- While the process of enrollment, creation of a database, and comparison between the template and the sample is common to all biometrics, there are many different forms of biometrics. Four of the most common are fingerprints, iris recognition, facial recognition, and voice recognition. Two of the more speculative forms of biometrics are hand geometry and gait recognition. The champion of all forms of biometrics is DNA analysis.

- Fingerprint-recognition technology is probably the most widely used and well known biometric. Fingerprint recognition relies on features found in the impressions made by distinct ridges on the fingertips. Fingerprint images are scanned, enhanced, and then converted into templates. These templates are saved in a database for future comparisons using

Fingerprint scanner

optical, silicon, or ultrasound scanners. Using fingerprints has seemed to work as a way of protecting privacy without too much inconvenience.

- Iris-recognition technology relies on the distinctly colored ring that surrounds the pupil of the eye. Iris-recognition systems usually start with a small camera that takes a picture of the iris. The picture is then analyzed to identify the boundaries of the iris and create a coordinate grid over the image. Then, the distinctive characteristics found in each different zone are identified and stored in a database as the individual's biometric template.

- Facial-recognition technology identifies individuals by analyzing certain features of the face. Typically, facial recognition compares a live person with a stored template, but it also has been used for comparison between photographs and templates. This technology works for verification and for identification. DeepFace, the facial-recognition technology developed by Facebook, is said to be 97 percent accurate, making it competitive with human-distinguishing capabilities.

- Voice-recognition technology identifies people based on vocal differences that are caused either by differences in their physical characteristics or from speaking habits. Such systems capture a sample of a person's speech, which is then converted to a digital format, and distinctive characteristics (such as, pitch, cadence, and tone) are extracted to create a template for the speaker. Voice-recognition technology can be used for both identification and verification.

- A more speculative form of physical recognition is hand geometry: a measurement based on the human hand; the width, height, and length of the fingers; distances between joints; and the shape of knuckles. Using optical cameras and light-emitting diodes that have mirrors and reflectors, two orthogonal, two-dimensional images of the back and sides of the hand are taken. Based on these images, 96 measurements are calculated, and a template is created. Hand geometry is a mature technology primarily used for high-volume time-and-attendance and access control.

- Gait recognition is an emerging biometric technology that involves people being identified purely through the analysis of the way they walk. Scientists in Japan have developed a system measuring how the foot hits and leaves the ground during walking. They then use 3-D image processing and a technique called image extraction to analyze the heel strike, roll to forefoot, and push off by the toes. Some say the accuracy in recognition is up to 90 percent—with the caveat that if you know you are being watched, you can change your gait.

- DNA analysis is, perhaps, the most accurate biometric method of one-to-one identity verification. Your DNA is everywhere you are and remains, through "shedding," after you go. DNA evidence has increasingly come to be used to exonerate the wrongly accused and convicted: Hundreds of such cases have been overturned, at least 20 of which involved people who had served time on death row. Currently, the government is free to assemble a template DNA national database of anyone who has ever been arrested for a crime.

Policy Questions and Concerns

- The use of biometric technologies poses a host of interrelated policy questions.
  - Can the biometric system be narrowly tailored to its task?
  - Who will oversee the program?
  - What alternatives are there to biometric technologies?
  - What information will be stored and in what form?
  - To what facility/location will the biometric give access?
  - Will the original biometric material be retained?
  - Will biometric data be kept separately from other identifying personal information?
  - Who will have access to the information?
  - How will access to the information be controlled?
  - How will the system ensure accuracy?
  - Will data be aggregated across databases?
  - If information is stored in a database, how will it be protected?
  - Who will make sure that program administrators are responsive to privacy concerns?
  - Can people remove themselves from a database voluntarily?
  - How will consistency between data collected at multiple sites be maintained?

- If there is a choice, will people be informed of optional versus mandatory enrollment alternatives?

- Some of the fears surrounding biometric information include that it will be gathered without permission, knowledge, or clearly defined reasons; used for a multitude of purposes other than the one for which it was initially gathered; disseminated without explicit permission; or used to help create a complete picture about people for surveillance or social control purposes.

- There also are concerns about tracking, which is real-time or near-real-time surveillance of an individual, and profiling, where a person's past activities are reconstructed. Both of these would destroy a person's anonymity. The following are some ideas about biometrics to consider.
  - Enrollment in biometric systems should be overt instead of covert.

  - Before one is "enrolled" in a biometric program, one should be made aware of that enrollment.

  - Biometric systems are better used for verification rather than identification.

  - We should prefer biometric systems that are "opt in," and require a person to consent, rather than those that are mandatory. While certain biometric applications (e.g., DNA for convicted criminals) might need to be mandatory, this should be an exception to the general rule of voluntariness.

  - Any biometric system should have strong audit and oversight programs to prevent misuse.

  - We need to be concerned about the security and privacy of a biometric database.

- But all of this pales next to the larger question of who gets to decide: Should citizens have a right to control their extremely sensitive biometric data?

- In one sense, the answer seems like it should be obvious: If anyone can take a photo of you on the street without your permission, why can't the government? On the other hand, it *is* the government.

- Today, however, the decision to move forward with biometrics is not the subject of wide public debate. In 2014, the FBI started to use a Next Generation Identification biometric database with 14 million face images. Current plans are to increase that number to 52 million images by 2015, with more images to be collected in the future.

- Biometric technologies are likely to be of great value in creating secure identification. But to be useful and acceptable, they need to be privacy- and civil liberties–neutral. They can, and should, be designed with appropriate protocols to ensure privacy before they are implemented.

Questions to Consider

1. Biometrics is a better form of security than passwords, typically. Do you prefer to use biometrics or passwords? Why?
2. Which type of biometrics makes you most unconformable? Which makes you least uncomfortable?
3. Should the government have a DNA database of everyone ever convicted of a crime? What about a DNA database of everyone ever arrested?

Hacking, Espionage, and Surveillance

The subject of this lecture is the surveillance of American citizens by a foreign government through cyber means. In this lecture, you'll learn about three aspects of this issue. First, you'll consider why foreign surveillance might be more common today in cyberspace. What is it about the domain that enables surveillance? Second, you'll learn about how cyber intrusions and surveillance happen. Third, you'll consider what this all means in terms of the surveillance of Americans.

Foreign Surveillance

- Only a few years ago, the topic of foreign surveillance on American soil would have been a subject of little concern. Such spycraft, when it occurred, would have been limited to instances of physical or electronic surveillance that were few and far between. This was mostly because virtually all personal surveillance required a physical presence in the United States as a condition of successful action.

- Today, that paradigm has changed. The Internet telescopes time and space. It allows almost instantaneous action at a distance. That's a sea change in our conception of surveillance.

- The history of human interaction is, essentially, one of the increasing distance at which our interactions occur. Over time, the necessity for close proximity has weakened.

- Cyberspace is a quantum leap in that direction. Action in the cyber domain occurs at the speed of light and crosses immense distances almost instantaneously.

- Whether the object is warfare, terrorism, espionage, or crime, it is no longer necessary for the malevolent actor to be anywhere near his or

her objective. As a consequence, America today is more vulnerable to foreign surveillance and espionage than ever before.

How Cyber Intrusions and Surveillance Happen

- How does a foreign government get into your computer? Typically, the attack arrives through an email message, or some other innocent form of communication, often from someone in your address book (and you're in the sender's address book, as well). Often, the message consists of just a website address—a hyperlink for you to click on. Such links will take you to web pages where embedded malware lives. And that could be the start of your computer being compromised.

- More than 200 billion emails are sent every day, some of which are the source for roughly 150 million different phishing attacks (in which the bad link is the bait and you are the fish). Even if only a tiny fraction of a percentage of these attacks succeeds, it still means that a massive number of people are affected by these types of attacks.

- Still, that kind of simplistic attack is not what a moderately cautious, sophisticated user should be afraid of. A more subtle type of attack is a malicious intrusion called a Trojan horse (or, simply, a Trojan). They are called Trojans because, typically, the malware is hidden inside a program that looks like an innocent piece of information—just like the famous Trojan horse that had Greeks soldiers hidden inside.

- Usually, an attack begins with the simple Trojan communication. Often, it is just an email to someone. This is often called a spear-phishing email, because it targets a specific individual or recipient, much like a spear used to catch a particular fish.

- Instead of a generic message that fits almost anyone, it will have a message designed specifically for you (or a narrower target group). These spear-phishing emails are designed to appear as though they have come from an innocent source, but they will have a malicious program hidden within—either in the email itself or possibly in an attachment.

- When the unsuspecting recipient clicks on the attachment, the malware begins the automated download of a controller program. This program then opens up a backdoor communications channel, allowing outside individuals to access the programs that control the target's system.

- When the communications open up, the attackers flood the system, much like a tank brigade moving through the breach in a defensive line. Some of the attackers create new breaches; others use their position to promote themselves within the system and give themselves authority to access all of the data available. If it is a quick hit-and-run attack, they begin removing information from the target system, such as your login codes or financial data.

- The intrusion doesn't have to be a quick hit-and-run. There is another class of attacks that are called, generically, advanced persistent threats (APTs), which are intrusions that are developed over time, using sophisticated attack methodologies that are directed at specific targets. Once inside a system, the APT might stay resident in the target for a long period of time and, in effect, make the target computer vulnerable to continuous monitoring from the outside.

- These types of intrusions are common forms of surveillance operated by foreign governments (and doubtless by our own government overseas).

- An example of a successful spear-phishing expedition was the Chinese attack on the U.S. Office of Personnel and Management (OPM). Sadly for the U.S. government, OPM manages the security clearance process for federal employees. As a result, it's thought highly likely that every file associated with the OPM-managed security clearance process since 2000 was exposed.

- That's data on roughly 22.1 million people who work in America's security community, and it includes 1.1 million sets of fingerprints, as well as the detailed financial and health records of all these employees and their spouses. It is the greatest espionage surveillance coup of all time.

- With the data from this intrusion, China now knows the names of almost everyone in America who has a security clearance. That means two things: First, it makes it much more difficult for the United States to stage covert operations when the identity of many of its spies is already known to the Chinese. Second, it means that the Chinese now have information about those who work in our intelligence and law-enforcement communities that they can use to extort cooperation from them upon threat of public disclosure.

The Surveillance of Americans

- The espionage and surveillance of average Americans is usually just a tactic aimed at a larger strategic objective. Chinese attacks on OPM, for example, are stepping-stones to bigger and better things. It is a source

of both traditional national security intelligence and, in the end, a means of stealing intellectual property and advancing the Chinese economy.

- The American security companies Mandiant (now owned by FireEye) and Crowdstrike have identified two arms of the People's Liberation Army—known by their Military Unit Cover Designators as Units 61398 and 61486—as special operations aimed at hacking foreign economies.

- It appears that these units are tasked with the object of attacking and intruding into the system and database of business enterprises and research institutions in order to steal trade secrets, technical talents, and any useful data from and through the Internet.

- In Unit 61398 alone, several hundred operators worked for more than 5 years, penetrated more than 140 known corporate and government systems, and stole more than 6.5 terabytes of data, according to FireEye. Nearly 90 percent of the victims were in English-speaking countries, and nearly 98 percent of the attacks were based on systems using a simplified Chinese language input. The Chinese government denied everything.

- The FBI warned U.S. health-care companies specifically that malicious threat actors were targeting them in an attempt to steal intellectual property and personally identifiable information. However, FireEye revealed that a Chinese hacker group also had systematically stolen data and information of the U.S. medical device manufacturers and pharmaceutical companies.

- How should we assess these Chinese activities? Are they significant threats? Should we credit the routine denials that China makes, disclaiming responsibility?

- First, there is little basis for accepting Chinese denials of awareness and responsibility. Nobody who seriously studies the issue doubts that the attacks on American systems are part of a systematic campaign that could not really occur without Chinese state approval.

- Second, we should think about how one should respond to this sort of activity, if at all. The response, if any, must come from the U.S. government. The American private sector has virtually no leverage to use to modify Chinese behavior.

- To date, we've seen at least two different types of U.S. government action in an effort to restrain Chinese surveillance and espionage. The first is the deployment of the American criminal system.

- For example, in one well-publicized instance, the Department of Justice indicted five Chinese military hackers who were believed to be part of Unit 61398. They were charged with computer hacking, economic espionage, and other offenses directed at six victims in the U.S. nuclear power, metals, and solar products industries. This was the first time that charges were brought for cyber offenses against individuals presumed to be acting on behalf of a nation-state. China did not agree to extradite the five individuals, and there seemed to be no real prospect that they would be brought to trial.

- So, the U.S. government turned to a broader tool: economic sanctions. President Obama issued an executive order: "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." Under this directive, the Treasury Department was authorized to freeze the assets of any individual or entity found to "be responsible for or complicit in … cyber-enabled activities … that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."

- In announcing this policy, the White House said that hackers and their sponsors from China, Russia, and Iran are the targets of the sanctions. However, at least initially, no sanctions were actually imposed; it seems that the White House hopes that the mere threat of sanctions will cause a change in behavior.

Questions to Consider

1. Typically, we fear surveillance by our own government more than by a foreign government. Why?
2. What do you do to protect yourself against a cyber intrusion?

Local Police on the Cyber Beat

Local police are the biggest collectors of surveillance data. In this lecture, you'll learn about the most prevalent forms of police surveillance today: the use of video cameras for anticrime surveillance and license plate readers, which are used for more prosaic things, such as the enforcement of red lights and speed limits. Then, you'll learn about the newest issue of police surveillance—body cameras—and some of the privacy issues they pose. Furthermore, you'll learn about how the New York Police Department, the largest in the nation, is pulling all of its data collection together.

Fixed Surveillance Cameras

- There can be little doubt that fixed surveillance cameras—or closed-circuit television (CCTV)—are effective tools for some purposes. This is especially so for retrospective investigations. When a crime has occurred, surveillance video that has been taken and stored can be pulled up and analyzed.

- After four Muslim terrorists detonated bombs in London's Underground and on a bus in July 2005, the suspects were quickly identified from CCTV footage taken at Luton station, where they had entered the subway system. The London attacks also demonstrated another important aspect of the proliferation of CCTV: Most of the video is maintained by private sector actors rather than by the government.

- Soon after the four suspected attackers were identified in London, the U.K. authorities were able to backtrack their movements over the days prior to the attack. CCTV video showed, for example, one of the men arguing with a cashier at a gas station, contending that he had been shortchanged. Other video seemed to suggest that the bombers had done a dry run through the Underground as a means of reconnaissance in the days preceding the attack.

- The London experience was not unique. After the tragic bombing at the Boston Marathon in 2013, a key piece of evidence was from a CCTV camera operated by a department store across the street. This camera showed an attacker leaving a black backpack next to a mailbox in the precise location of the explosion.

- But do CCTV cameras work prospectively? That is, do they reduce crime by deterring bad conduct? You might think that the answer would be yes, based on the theory that surveillance cameras would deter potential offenders. However, the evidence is mixed.

- In London, for example, the cameras are so plentiful that they are called a "Ring of Steel" around the city center. But many residents question the effectiveness of London's system. Only one crime was solved for every 1,000 cameras, according to a police report for a recent year. At the same time, CCTV cameras were costing authorities hundreds of millions of dollars per year, according to the civil liberties group Big Brother Watch.

- In the United States, the Urban Institute reviewed the use of CCTV in three cities—Baltimore, Chicago, and Washington DC—in its report "Evaluating the Use of Surveillance Cameras for Crime Control and Prevention."

- In Baltimore, public surveillance cameras installed in the 50-block CitiWatch section reduced violent crime by 23 percent between 2003 and 2008, according to the report. By contrast, in Chicago, where cameras were put into two communities, only one saw a reduction in crime, while there was no visible effect in the other. Washington DC seems to have identified no appreciable change in criminality after cameras were installed.

- Supporters of CCTV usage will tell you that the reason cameras didn't work in DC is because of the privacy and civil liberties restrictions placed on them—restrictions that the community as a whole thought were

essential. Opponents will tell you that it is more than just surveillance; it's the prospect of its pervasiveness that scares them.

- Civil liberties activists are concerned about how the technology could be abused. Imagine, for example, cameras in far-flung cities all connecting to the same database so that a person's movements can be tracked across states—maybe to follow a political protestor instead of a terrorist. Another factor worth considering when we think about CCTVs is the trade-offs in surveillance and security systems.

License Plate Readers

- License plate readers are fixed cameras that have only a single object of interest: tracking vehicles. The technology for this is not new. Optical character readers are used to translate the image or picture of the license plate into a text that can be read and stored.

- Most of what happens with respect to collecting license plates is unregulated. After all, the police could sit at a toll plaza and write the plate number down by hand, so there really is no readily apparent privacy concern. The privacy interest arises when the collection becomes pervasive and systematic. And that's exactly what is happening.

- *The Wall Street Journal* reported that the Justice Department was building a national database to track, in real time, the movement of vehicles around the United States. The program is said to have begun innocently enough, with an initial focus on tracking cars along the Southwest border to follow the movements of drugs and drug money. It was housed at the El Paso Intelligence Center in Texas, a law-enforcement intelligence center that is staffed 24 hours per day. But today, the program is national in scope.

- The Department of Homeland Security has its own database. U.S. Customs and Border Patrol personnel collect information on land-border traffic, amounting to hundreds of millions of license plates. And New York City has long collected the license plate of every car entering or leaving Manhattan.

Body Cameras

- In the wake of tragic events in Ferguson, Missouri—and elsewhere—where police were reported to have killed unarmed African Americans in the course of street patrols and other law-enforcement activity, policy makers across the country increasingly called for the use of police body cameras.

- This was a new way of recording police interactions with the public. The idea was that if these interactions were observed, they were more likely to occur in a lawful and appropriate manner. In other words, we think that surveillance of the police might make the authorities' performance better.

- In highly charged circumstances, the recording of law-enforcement interactions with the public might just as readily support the contentions of police officers, who sometimes perform their job under fraught conditions.

- Body cameras are proliferating around the country. Large cities, including New York and Washington DC, were buying them, as were smaller communities. Some estimates projected that 10 percent of the police nationwide might end up wearing body cameras.

- We already see anecdotal evidence that the video record is helping to resolve he-said, she-said disputes between the police and private citizens. In New Mexico, a police helmet camera captured the fatal police shooting of a knife-armed homeless man as he was turning away, demonstrating an instance in which police likely overreacted.

- Conversely, in Celina, Texas, two cameras told different tales of the arrest of a man high on heroin and helped resolve a dispute over whether the officer had used excessive force. One camera was on the police car's dashboard, and from its vantage, the officer's takedown of the suspect might have been viewed as excessive. But the body camera revealed a much different view: The suspect threw a punch at the officer in an attempt to escape and only then was dragged to the ground.

- Researchers from the University of Cambridge's Institute of Criminology have published a study showing that not only do the cameras protect the public from the police, but the cameras also protect the police from the public.

- In Rialto, California, reports of police use of force fell by 59 percent after local officers wore body cameras for one year, and there was an even more significant drop in public complaints against the police, which declined by 87 percent compared to the previous year.

- Some privacy issues still exist, and rules about protecting both witnesses and police must be established and tested.

The New York Police Department

- New York's Lower Manhattan Security Coordination Center is operated by the New York Police Department (NYPD). It monitors more than 6,500 security cameras south of Canal Street, which is the northern boundary of the area that broadly encompasses Wall Street and the New York City Hall complex.

- Some of these cameras are fixed; others are mobile. In many cities, police cameras are not connected to a central feed, but New York's cameras are networked so that they are viewable, in real time, by officers in the Lower Manhattan Security Coordination Center. In other words, they are centrally monitored: watched, analyzed, and responded to.

- The project uses feeds from private and public security cameras so that the information is collected not only from the city cameras but also from department stores' and office buildings' CCTV. And all of it is monitored 24 hours per day.

- The NYPD also makes use of license plate readers, which capture more than 2 million license plates every day. Other sensors available to the police measure radiation, chemical releases, biological contaminants,

and explosives—and all of that data gets fed into the central monitoring system.

- Apart from this, New York police also have a variety of electronic databases at their disposal. These include arrests, complaints, 911 calls, parking summonses, and vehicular moving violations. The Lower Manhattan Security Coordination Center aggregates digital copies of all of this information into a single database.

- The system processes 1.5 billion records and issues alerts as they are triggered. And when the system issues these alerts, the police react. Whatever the source of the alert, the NYPD first assesses the information and then decides whether or not to act—and, if they act, in what way.

- New York is not insensitive to the privacy concerns about this program. It has data storage rules that require deletion of some data after a fixed period of time (typically 30 days). The city also has an audit function to track the use of the system so that it is applied only to legitimate public safety issues.

- Compared to what came before it, this system represents a significant upgrade in analytical capacity and capability for the NYPD. Reflecting the new technology and tenor of our times, it very likely that it is also the wave of the future.

Questions to Consider

1. Surveillance by the national government gets all the attention, but it is much less in volume than surveillance by local police. What causes the difference in attention?
2. What do you think of the New York system for lower Manhattan? Is it good security or Orwellian?
3. Think about how Washington DC controls cameras with rules set by civilians. Is that the right way to make decisions, or do civilians underestimate the need for security?

Geolocation: Tracking You and Your Data

Geolocation is a tracking phenomenon that identifies where a person is physically. As this lecture surveys the field of geolocation, it will identify three separate concepts that form a useful framework for the discussion. They relate, broadly, to the manner in which geolocation information is collected. In some instances, we volunteer that information to the world around us. In others, geolocation data is collateral information that is necessarily collected as part of some other process, such as making a phone call. A third way of collecting geolocation data is through surreptitious means.

Voluntary Geolocation Data Collection

- Some people deliberately share their geolocation by formally tagging their location and "checking in" at various places on social media sites. If you use an app like Foursquare or Swarm, you are purposefully broadcasting where you are. And it is pretty easy to accumulate that data and use it to draw a picture your activity.

- For example, Raytheon has developed something called Rapid Information Overlay Technology (RIOT), which uses only publicly available data from social media programs like Instagram, Facebook, Foursquare, and Koala. With that information, you can draw a detailed picture of a person based on where he or she goes. Raytheon understands the power of this kind of analytic tool—and the peril. That's why it describes the RIOT tool as privacy protective.

- One of the common tools that system integrators often use as a means of ameliorating privacy and civil liberties concerns is the tool of partial masking, or pseudonymity. By scrubbing linked data of personally identifiable information—but still making it capable of being correlated and analyzed—you can create a two-step process that is thought to be more robust in protecting privacy.

Foursquare is a mobile app that broadcasts your geolocation.

- At the first step, data that is scrubbed of identity markers is linked together in patterns. Only when those patterns meet some threshold of concern (and, typically, when some third party or supervisor verifies that the threshold has been exceeded) is the anonymity of the data removed and identifying information added back in. In this way, large volumes of innocent collateral data can be collected and sifted in an automated fashion without—it is said—threats to privacy. Of course, to rely on that system, you have to trust the process.

- Geolocation is essential to navigation functions, such as Google Maps. That's the type of functionality that you can't turn off and still navigate, so the only way to avoid exposing your location data is to not use the function at all.

Necessary Geolocation Data Collection

- Some geolocation functions are, for all intents and purposes, an essential component of modern-day life. When that happens, then the sort of surveillance that in other contexts might seem only a bit creepy can become pretty scary and even downright authoritarian.

- Think, for example, about your cell phone—not all of the supersophisticated location apps that you could do without, but rather the phone itself and the voice and text communications that are probably at the core of your personal mobility (and your personal connectivity).

- These features also allow the phone company to know exactly where you are all the time. Your cell phone is constantly reporting your location to the nearest cell towers. That's how the telephone system knows where you are so that it can connect a call to you. The phone company keeps records of where your cell phone is (or was). That means that they know where you are right now and also where you've been.

- Maybe you're not worried about what your phone company knows. But what if they sell it to some commercial advertiser? Or what if the government issues a subpoena and collects all these records?

- The issue is highly contentious. But the law says that the Fourth Amendment does not protect information you share with a third party. So, when you "voluntarily" broadcast your location to the cell phone company or Facebook, that means there is no Constitutional rule that prevents them from turning around and giving the information to the government.

- That's a pretty odd definition of "voluntarily." That kind of implied consent has a very forced feel to it. We can't turn the geolocation part of the cell phone off—at least not if we want our cell phones to work. And we can't really quit society. Our consent is, in effect, coerced.

- That's why a few courts around the country are taking a different vie, and extending the law governing warrants to cover cell tower records. They are saying that in the absence of a warrant based on probable cause, the government can't secure these historical records.

- And that extension, which naturally limits police methods, brings with it problems of a different sort. Sometimes, geolocation cell tower data can

be powerful evidence of criminality. In one case, cell tower data located the defendant's mobile phone in close proximity to six different armed robberies.

- As a society, we need to choose how much (or little) access we want to give the government to geolocation data. The basis for this choice comes down to a rough form of cost-benefit analysis.

- If we think the value of the positive uses of a technology are great enough, then we will deploy it while trying to manage its use through warrant requirements, or data retention rules and the like.

- If we are concerned that a technology provides too much surveillance power to the government, we often consider banning the technology altogether. But that step isn't always possible if we are too dependent on it. That is why some groups always fight so hard to prevent a new technology from coming online—not because initial uses are so abusive, but because a step down that technological path can't easily be untaken.

Surreptitious Geolocation Data Collection

- At least in the case of cell phones, when it comes to the collection of geolocation data by the government without your knowledge or consent, we could point to your implicit agreement through your use of the company's geolocation technology. But what happens when the government starts tracking you without your knowledge?

- One important example of this is exemplified by a tracking system known as StingRay. When a StingRay tracking device is turned on, it pretends that it is a cell phone tower. It simulates the "call out" from the tower to nearby phones (even when they are not on). Those phones, in turn, respond to the StingRay by reporting in their phone number and a unique electronic serial identification number.

- According to the nonprofit civil liberties organization in Washington known as the Electronic Privacy Information Center (EPIC), government investigators and private individuals alike can use StingRay and other "cell

site simulator" technologies to "locate, interfere with, and even intercept communications from cell phones and other wireless devices." EPIC says that the Federal Bureau of Investigation has used such cell site–simulator technology to track and locate phones and users since at least 1995.

- According to *The Wall Street Journal*, the U.S. Marshals Service flies planes carrying devices that mimic cell phone towers—in order to scan the identifying information of Americans' phones—as it searches for criminal suspects and fugitives. Under this program, the government collects data from thousands of mobile phones. Along the way, it also collects (and then, it says, discards) data on a large number of innocent Americans.

- The Justice Department justifies the phone records collection program by arguing that it is minimally invasive and an essential way to attempt to track terrorists and criminals. Its main virtue, from the government's perspective, is that the program eliminates the need to go to phone companies as an intermediary in searching for suspects. Rather than asking a company for cell tower information to help locate a suspect—a process that law enforcement has criticized as slow and inaccurate—the government can get that information itself.

- Naturally, others see that as problematic. Christopher Soghoian, chief technologist at the American Civil Liberties Union (ACLU), characterizes it as "dragnet surveillance." He says that StingRay in the air is "inexcusable and it's likely—to the extent judges are authorizing it—[that] they have no idea of the scale of it."

- One recurring theme in contemporary issues of law and technology is the balance to be sought between secrecy and transparency. It's important for American citizens to know what their government is doing. On the other hand, it's clear that the disclosure of certain surveillance techniques can significantly affect the secrecy of them, perhaps resulting in the technology getting into the wrong hands.

- The U.S. government is anxious—some might say desperate—to keep StingRay's technology out of the hands of nongovernment actors. To

that end, whenever they're asked to produce the equipment in court, they dismiss the case rather than disclose how the StingRay actually works.

- Either the government's use of new technologies in the public sphere will have to be fully disclosed and made subject to adequate oversight or the police are going to have to give up such surveillance and tracking tools if they can't withstand the scrutiny that comes with its use in a free society.

- One small step in the direction of reconciling the conflict is that the Department of Justice (DOJ) has said that as a matter of policy (not legal obligation), federal law-enforcement officers will seek warrants before using a StingRay. That's probably a sound result, but note that the DOJ doesn't bind the state and local law enforcement who use StingRay.

- The ACLU's Chris Soghoian points out that there is yet one more reason why the secrecy surrounding StingRays is problematic, at best. The idea is that if the FBI can use Stingrays, then so can our enemies.

Questions to Consider

1. Think about all the places you go every day. How well does that travel pattern describe you?
2. Where someone is located is often vital evidence of a crime. How can we allow the government to use that information for security without intruding on privacy?
3. Does it matter whether the information is collected by your cell phone company, for example, first and then shared with the government instead of by the government directly?

Internet Surveillance

The topic of this lecture is how individuals are tracked on the web. In this lecture, you'll learn about how the web surveillance program works in the United States, why it was set up the way it was, and how the government says it is protecting privacy and civil liberties through its surveillance. Along the way, you'll learn what some critics of the program say about it, as well as what some of its defenders say.

The Government Surveillance of the Web

- The government surveillance of the web goes by many names. One code name that is often used is PRISM. Another name for it is the Section 702 program, after Section 702 of the Foreign Intelligence Surveillance Act, which authorizes the collection of some private communications. The Section 702 name is a bit more precise, because it relies on a clear definition in the law. The PRISM program is just a subset of it.

- Section 702 has its origins in the president's terrorist surveillance program, which was initiated in the immediate aftermath of the 9/11 terror attacks. Although undertaken on the president's order, one of the oddities of this program—and the controversy that came to envelop it—is that Congress fully discussed and authorized it.

- But that authorization did not happen in 2001 when, in the wake of the attacks, Congress might have been overwrought and emotional. Rather, the law was adopted and amended twice later in the decade, after the program had been initiated on the president's own authority.

- First, Congress adopted a temporary measure known as the Protect America Act in 2007. Then, it passed the FISA Amendments Act of 2008. This is the statute that includes the new Section 702. That's not to say that the program functions exactly as Congress anticipated. But

America—and the government—went into this program with its eyes wide open.

- Under Section 702, the U.S. attorney general and the director of National Intelligence may jointly authorize surveillance that targets people who are not "U.S. persons," a term of art in the intelligence community that means people who are American citizens or permanent resident aliens. So, the targets of Section 702 surveillance should not be U.S. persons.

- Section 702 only allows the government to acquire foreign intelligence by targeting non-U.S. persons "reasonably believed" to be outside U.S. borders—in other words, foreigners on foreign soil. It is expressly against the law to try to collect information from targets who are inside the United States—whether Americans or foreigners—or to deliberately target the collection of American web communications.

- The law also requires the government to develop "targeting procedures": These are the steps the government needs to take to make sure that there is a reason to believe that the target is outside the United States. This is sometimes difficult. After all, your cell phone might not go with you when you go overseas. In the end, the government must get these targeting procedures approved by the Foreign Intelligence Surveillance Court so that the court approves the system of targeting rather than the individual targets themselves.

- To conduct this surveillance, the government can compel assistance from Internet service providers and telephone companies in order to acquire foreign intelligence information—that is, information relating to a foreign espionage program or international terrorism.

- And it's pretty clear that the government pays a pretty penny to all the communications companies that participate in PRISM and provide data. The payments range from 250 dollars to nearly 400 million dollars annually, according to *The Washington Post*. Some advocates suspect that as a result, surveillance turns from a legal obligation to a source of income.

The United States government collects data on some private communications that take place on the Internet.

Why the Program Works

- Why does this program work? After all, couldn't foreigners who want to avoid U.S. interception simply avoid sending traffic through U.S.-based servers? In theory, yes. In practice, not really.

- Much of the world's electronic communications pass through the United States. Because the automated protocols that direct the information flows on the network tend to find the cheapest and quickest route, it turns out that a large majority of Internet traffic crosses American borders.

- This infrastructure superiority is America's home-field advantage. It gives U.S. intelligence analysts the opportunity to intercept the communications of foreign targets as their electronic data pass through the United States.

- It's been estimated that anywhere from 25 percent to 80 percent of global Internet traffic passes through the United States. But other global players are moving to expand their own infrastructure and challenge American dominance, in part because of continuing disclosures about

how U.S. authorities have become global traffic cops—and even spied on allies, as well as enemies.

- What Congress originally authorized is a program that cannot intentionally include any U.S. persons or anyone (whether American or foreign) who is located in the United States. And it could be targeted only at the collection of foreign intelligence information—that is, information relating to a foreign country's efforts against the United States (or for counterterrorism purposes).

- But that isn't the whole story, because foreign intelligence communications might be intermingled with the casual, everyday communications of U.S. persons. The reality is that a fair amount of information about Americans is collected.

Privacy Protections

- If we are going to collaterally collect information about Americans in a program designed to monitor foreigners, what's to keep that information from being misused?

- When information is collected about an American—whether collaterally as part of an authorized investigation or inadvertently as the result of a mistake—the government is required to "minimize" that information. The word "minimize" means to limit its collection of the information, to retain it (if at all) only for a limited period of time, and to use information about Americans only in narrowly defined circumstances. It also might mean deleting the information entirely.

- As with the targeting procedures, these minimization procedures are also approved by the FISA Court—but, again, the approval is for the system of minimization, not each individual case.

- So, for example, under these minimization procedures, agencies such as the NSA, CIA, and FBI are not allowed to unilaterally sift through the data they've collected. Rather, they must demonstrate a reasonable

likelihood that targeting a particular item in the information collected is going to result in the development of foreign intelligence information.

- In other words, the rules in place limit when an American can be targeted for examination and how long data about an American can be retained before it ages off and is deleted.

Support for and Critiques of the Program

- There is a fair amount of support for the Section 702 program. By many accounts, the program has been a success in the development of foreign intelligence. It has proven to be flexible and produced an increase in the number of suspected foreign agents, whom we can target and monitor.

- The Privacy and Civil Liberties Oversight Board—a bipartisan panel within the executive branch that reviews actions the executive branch takes to protect the country from terrorism and also monitors civil liberty concerns—has reported that more than one-quarter of NSA reports on international terrorism include information that is based in whole, or in part, on data collected under the Section 702 program.

- Although the details are classified, the board also has said that the program has played a role in discovering and disrupting specific terrorist plots aimed at the United States by enabling the government to identify previously unidentified individuals involved in international terrorism.

- Some critics of the program dispute this claim. For example, one investigation that the government publicly said was aided by PRISM was the case of Najibullah Zazi, who had planned to bomb the New York City subway. The *Guardian* newspaper interviewed several people who were involved in the case and reviewed U.S. and British court documents, concluding that the investigation began with "conventional" surveillance methods rather than from leads produced by NSA surveillance.

- We really have no good data on how much incidental collection there is about U.S. persons. We do know (thanks to a board report) that, at one time, 198 U.S. persons were identified as legitimate targets of collection.

But the real issue is how many are collected as collateral to the general foreign intelligence mission.

- After all, if the volume of incidental collection overwhelms the useful data on terror threats, then we might be skeptical about its efficacy. But right now, we just don't know.

- The major criticisms of the program are far more fundamental. For example, some worry that the 702 program is, in effect, creating a vast storehouse of data.

- By far the largest complaint about the Section 702 program is that American data is retained—at least some of it. Under current rules, when the U.S. government is targeting someone abroad, it is not required to discard the incidentally collected communications of U.S. persons if authorities conclude that those conversations constitute foreign intelligence. In that event, even conversations by or about Americans can be retained.

- And the threshold for targeting an American within the data collected is relatively low. To search through the data collected for an American, all that is needed is a determination that the search is reasonably likely to return foreign intelligence information.

- One criticism, voiced by a Presidential Review Board as well as many members of Congress, is that Section 702 collection on Americans is a category mistake. The program, they argue, is appropriate without individual case supervision and a warrant requirement precisely because it targets non-Americans. So, when the communications of Americans are targeted, they contend that the probable cause and warrant requirements should apply—that the government should not be able to get through the back door of foreign surveillance evidence against Americans that it could only normally get through the front door of a warrant with judicial approval.

- For that reason, there have been efforts in Congress to amend the law to prohibit the NSA from searching its databases for information on Americans without a warrant based on probable cause, issued by a court. Thus far, those efforts have failed.

Questions to Consider

1. According to the Privacy and Civil Liberties Oversight Board, the Section 702 program has been of some real use to government counterterrorism efforts. Outside reviews by the press disagree. How do we resolve this? Is it a question of historical fact or of judgment? And if it is judgment, whose judgment do you trust?
2. The Section 702 program needs to be renewed periodically by Congress. If you were a representative or senator, would you vote to renew it? Why, or why not?

Metadata: Legal or Not

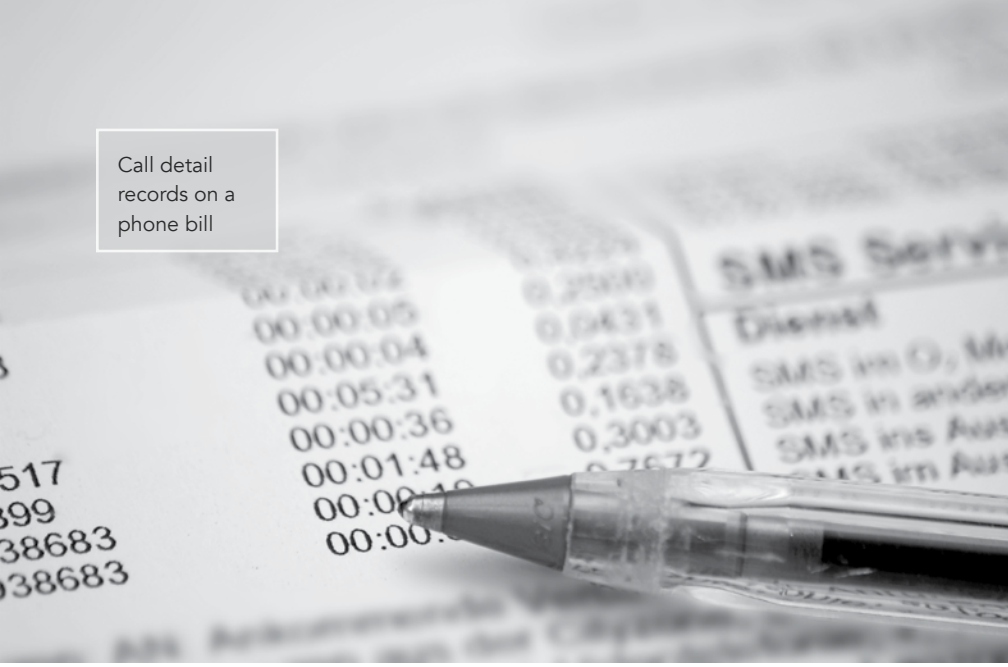
The U.S. government has collected the telephone records of everybody in the world, including Americans. One government surveillance program that you'll learn about in this lecture collects something called metadata (data about data)—whom you call, when you call, and for how long you talk—instead of the actual content of the communication, such as what you say to the person. The program is known as the Section 215 program, after the section of U.S. law that authorizes it. Or does the law authorize the program? The legal jury, as you'll learn, is still out.

The Section 215 Program

- The Section 215 metadata collection program arises from the USA PATRIOT Act, which was signed into law in October 2001 and gave rise to an accompanying series of orders issued by the Foreign Intelligence Surveillance Court (FISC).

- The orders require telephone companies operating in the United States to provide the National Security Agency (NSA) with what are known as call detail records: the detailed information of the sort that typically appears on your telephone bill, including the date, time, and duration of a call, as well as the phone number to which the call was placed or from which it was received.

- As described by the Privacy and Civil Liberties Oversight Board, this Section 215 metadata was to be maintained by the NSA in a centralized database. NSA analysts can search the database with a query—an input of a search term, such as a phone number—but they may do so only if one of 22 designated NSA officials first determines that the query is based on a reasonable, articulable suspicion that the phone number at issue is associated with terrorism.



Call detail records on a phone bill

- Once a reasonable, articulable suspicion-based search is approved, NSA analysts are allowed to do what is known as, "contact chaining," the practice of retrieving not only the phone numbers in direct contact with the number in question (known as the "first hop"), but also all the contact numbers associated with the numbers identified in the first hop (including second-hop and even third-hop numbers). That becomes a huge field of search to survey.

Is the Program Working?

- The bipartisan Privacy and Civil Liberties Oversight Board in the executive branch of the federal government—which reviews anti-terror programs advanced by the executive branch and also keeps an eye on civil liberties—conducted a full-scale review of the Section 215 metadata program.

- Nevertheless, the board's review did suggest that the telephone records collected by the NSA under Section 215 had provided some value, primarily in two ways: by offering additional leads regarding the

contacts of terrorism suspects already known to investigators and by demonstrating that foreign terrorist plots do not have a U.S. nexus.

- New leads can help investigators confirm suspicions about the target of an inquiry or about persons in contact with that target. And identifying the nexus of a foreign plot can help the intelligence community focus its investigatory resources by avoiding false leads and channeling efforts where they are most needed.

- The review suggested that the Section 215 metadata program mostly duplicates the FBI's own lead-generating efforts. Then again, some of the value of the Section 215 program is in its negative information.

- The Privacy and Civil Liberties Oversight Board's review was generally skeptical of the usefulness of the program. For one thing, as the board said, the best justification for the government's routine collection of all telephone records is that it helps in cases where there is no threat to the United States—that is, in cases where there is no real foreign terrorism connection.

- We should, the board said, find it a bit strange and disturbing that for a program officially focused on collection about foreign terrorism, the best use of it is for non-foreign activities.

- Standing against this limited effectiveness, there are some who say that the 215 program provides grave potential for abuse by the government. And that is fair enough—the potential for abuse is quite realistic and plausible. But the Privacy and Civil Liberties Oversight Board found precious little evidence of actual abuse.

- But even when there is not any abuse, we might reasonably ask whether or not the potential for abuse—or the structure of the program—has implications for privacy and civil liberties. From that perspective, the concerns are more palpable. The idea that the government holds a database of this magnitude is quite daunting to many citizens, even if the data is used for the best of purposes.

- Telephone call records are powerful metadata in and of themselves. Whom you call, when you call, and for how long you talk creates a mosaic that can reveal the most intimate details of your life.

- And we know that telephone call data is not the only type of data that a government (or, for that matter, a commercial company) might collect. The panoply of publicly available data on private individuals is large and is growing larger every day.

- The concern with the Section 215 program, therefore, is not just with the collection of metadata, but also with the fear that, as the Privacy and Civil Liberties Oversight Board said, "when aggregated with other information and subjected to sophisticated computer analysis, the government's collection of a person's entire telephone calling history [will have] a significant and detrimental effect on individual privacy." This is exacerbated when the data is stored for a period of time in the government's database, where it can be rapidly accessed and searched.

Revisions to the Program

- In response to these concerns, Congress substantially revised the Section 215 program in a bill known as the USA Freedom Act, under which the law was changed to stop the NSA from continuing its mass phone data collection program.

- Two principle changes were made. First, instead of the data being collected in a government database, phone companies would retain the data in their own databases. And they would not be required to hold the data for any longer than their normal business practices require—typically around 12 to 18 months.

- Second, after the law took effect, the NSA would be able to obtain information about targeted individuals only after authorization from the FISA Court. And before a particular phone number was selected for analysis and targeting, the government would have to show the court a reasonable, articulable suspicion for why that phone number might be connected to foreign intelligence or terrorism.

- The most obvious civil liberty is that the government would no longer have a large-scale database on all Americans. Many think that the creation of such a database was a fundamental shift in America—one that might have changed it in a core, almost inexpressible way.

- Because the government has a monopoly on the lawful use of force in society, it also represents a unique threat to the liberty and privacy of citizens in ways fundamentally different than potential threats to privacy and civil liberties posed by corporate data collectors. We worry that the government's collection of data for one purpose might be, in the future, repurposed to less well-justified ends.

- Abuse tends to be insidious, proceeding incrementally. And even if the chances of it are remote, the fear of potential abuse could have indirect effects on freedom and liberty. For example, those who engage in controversial activities might not trust the government to honor their rights to privacy.

- We should not see the distributed system—where the phone companies keep the call data—as a complete panacea. For one thing, requiring the phone companies to hold the data increases the ability of commercial providers to analyze the data, and some people have even less confidence in commercial data aggregators than they do in the government.

- In addition, the requirement will inevitably make government less efficient at scrutinizing potential terrorist activity. That's a cost that comes with a distributed database that we will have to accept as the price of increased privacy. For now, Congress has made that judgment, in response to the concerns of the American public. Only time will tell if the choice was a wise one.

Is the Program Legal?

- The text of Section 215 (until it was changed by Congress) said that the government may secure an order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information."

- But the key to the Section 215 debate is the further requirement that "there are reasonable grounds to believe that the tangible things sought are relevant to *an authorized investigation* . . . to protect against international terrorism."

- Some read this language as one of great specificity—that "an authorized investigation" is singular in nature and targeted at a relatively particular individual or group of individuals. From this perspective, we have to put a fair amount of weight on the word "an"—the authorized investigation. This argues that the concept of relevance is a relatively narrow and directed idea.

- A law dictionary, for example, defines relevancy as "that which conduces to the proof of a pertinent hypothesis." You must, in this view, have an articulable hypothesis you are trying to prove or disprove—which suggests a narrow focus to the inquiry.

- By contrast, the government has argued (and convinced the FISA Court of its view) that there is a reasonable basis for believing that the bulk collection of metadata is likely to be relevant to an authorized investigation—that is, an investigation of foreign terrorist activity—more generally conceived.

- The Justice Department has argued that there is no a priori reason that "an investigation … to protect against international terrorism" should be narrow, given the far-flung and convoluted nature of terrorist organizations.

- In such a debatable legal issue, opinions differ on the meaning of the text. Section 215 of the PATRIOT Act authorizes the government to have access to business records for foreign intelligence purposes. It allows the government to obtain an order from the court for the production of "any tangible thing (including books, records, papers, documents, and other items)."

- Does this language mean that the government can get any tangible thing? If it does, then the statutory foundation of the bulk metadata

collection program is solid. On the other hand, consider that large, capacious, catchall phrases like "any tangible thing" are limited by the context in which they appear.

- Clearly, telephone records of individual calls would seem to be fairly within the scope of Section 215. They are a tangible record. But it is, at least, an open question of whether the entire database of every major phone company in the United States is a tangible thing. It might be that bulk collection of the telephony metadata database is very different from an ordinary business record.

- And what about the constitutionality of the Section 215 program? Doesn't the Fourth Amendment protect against this sort of governmental intrusion? Isn't the Section 215 program an unreasonable search and seizure? The answer, it turns out, is not terribly clear. For now, the courts are split on the question, as is the Privacy and Civil Liberties Oversight Board.

- The constitutionality of the Section 215 program might never be decided. In reaction to privacy concerns, Congress listened—and significantly changed the program.

Questions to Consider

1. The government's collection of metadata on telephone calls is widely considered the most troubling disclosure by Edward Snowden. Why? Do you agree, or are there other types of surveillance that are more problematic?
2. Would your views of the Section 215 program change if the historical record showed it to be more effective in discovering terrorists? How much more effective would it need to be to change your mind?

Technology Outruns the Law

Courts are frequently unwilling (and perhaps even unable) to adapt—in real time—to new questions that technology raises. This expresses the limitations of hierarchical means of analysis. The courts move slowly because they do not want to get the answers wrong. However, pressure is growing, and soon the courts might be obliged to act. In this lecture, you'll learn about the constitutional law system, including such aspects as expectation of privacy and consent.

Expectation of Privacy

- In *United States v. White*, the defendant was James White. A government informant, Harvey Jackson, had concealed a radio transmitter on his body, and law-enforcement authorities monitored the radio frequency the transmitter was tuned to. On eight different occasions, that hidden radio transmitted Jackson's conversations with White to law-enforcement authorities, including, on one occasion, at White's home.

- Based in large part on these conversations, White was criminally charged with drug trafficking. By the time of trial, however, Jackson had disappeared. The trial court let the government proceed by having the agents who had listened in on the conversation testify as to what they overheard. On this basis, the jury convicted White.

- But the accused drug trafficker then challenged his conviction. His main argument, on appeal, was that this new form of surveillance violated the Fourth Amendment to the U.S. Constitution. That amendment, part of the original Bill of Rights, says the following.
  - "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

- White argued that he had a reasonable expectation of privacy in his conversation with Jackson and that the government's surreptitious electronic interception of that communication violated his rights.

- On its face, White's argument had a bit of a problem. His statement that his expectation of privacy was violated runs square into the fact that the word "privacy" isn't in the amendment. What the amendment prohibits are searches and seizures—not all searches, only unreasonable ones.

- White's argument wasn't frivolous, though. For years, the Supreme Court had said the only way to measure "reasonableness" was by reference to law and legal restrictions. That changed in 1967, in a case called *Katz v. United States*.

- Charles Katz was a bookie who used a public pay phone to conduct his business. During its investigation, the FBI recorded Katz by attaching an eavesdropping device to the outside of the booth. Under the old style of law, because there was no physical intrusion into the phone booth, there would have been no legal barrier to what the FBI did and hence no unreasonableness to the search.

- But the Supreme Court nonetheless concluded that the FBI had violated the Fourth Amendment. In reaching that conclusion, the court modified, at least to some degree, how it defined what the Fourth Amendment protects.

- Justice John Marshall Harlan II's concurrence in the *Katz* case is the best expression of that change. He said the violation occurred because "an enclosed telephone booth is an area where, like a home … and unlike a field … a person has a constitutionally protected reasonable expectation of privacy … that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment."

- From this, Justice Harlan derived a two-prong test for an expectation of privacy: It existed if the individual "has exhibited an actual (subjective)

expectation of privacy" and society is prepared to recognize that this expectation is (objectively) reasonable.

- The court was not unanimous. In dissent, Justice Hugo Black said the Fourth Amendment was meant only to protect things from physical search and seizure and that it had no relevance to personal privacy. Black's losing argument in the *Katz* case took on new importance when technology began to render irrelevant the walls of a phone booth.

- Still, in the *Katz* opinion, you can see the nature of White's argument a few years later. In the apparent sanctity of his own home, the suspected drug dealer was surreptitiously recorded with the help of a miniature transmitter. By engaging in this conversation in a private space, White's attorneys argued, he was manifesting a subjective expectation that the communication with Jackson was also private.

- But White lost. The court said that White had no right to assume that Jackson would keep their conversation confidential. He could talk with the police if he wanted to. In other words, White's expectation of privacy did not rise to a reasonable expectation that his coconspirators would not rat him out to the police.

- The evolution in the law leading to Jack White's drug-related conviction goes a long way to explaining why, at least for now, constitutional law has little role in regulating the collection of internet and telephone data about an individual.

- When you give someone information, you lose control over how it is disposed of. This principle, soon to be called the third-party doctrine, was extended to the idea of personal data in two cases in the 1970s, *United States v. Miller* and *Smith v. Maryland*.

- In each, the question was, in effect, as follows: Does an individual have any constitutional protection against the wholesale disclosure of personal information that has lawfully been collected by third parties? And, in particular, could an individual use his or her Fourth Amendment

rights to prevent the government from using data it received without a warrant from a third-party collector?

- In both cases, the court answered with a resounding "no." Relying on the reasoning in cases like *White*, the court said that one has no constitutional rights to protect information voluntarily disclosed to others.

- One of the oddities of these two cases is that they are quite old, arising before personal computers existed and before there was much concern with wholesale collection of personal information. That hasn't stopped courts from applying the third-party doctrine in the modern context.

Consent

- Consent solves most of our constitutional problems with government search and seizure. If you give your consent to a police search, then, almost by definition, the search is reasonable. Provided that you are not coerced into giving your consent, then a citizen's decision to permit the government to scrutinize his or her actions is an authorization.

- In an ideal world, consent would be the bedrock of such authorizations. The idea of consent is a core of democracy and, in many ways, is a barrier to unreasonable government surveillance. The corollary is that in the absence of consent, surveillance would not generally be permissible. But here our theory runs into the relatively narrow definition given to consent by current court interpretations.

- The case of John Gilmore gives us a good sense of the issue. Gilmore was a civil liberties activist who sued the United States. He wanted to be able to fly on airlines without showing an identification document, such as his driver's license.

- Gilmore lost his challenge in a case that goes by the title of *Gilmore v. Gonzales.* The Ninth Circuit Court of Appeals decided the matter on two grounds: one relating to reasonableness and another relating to consent.

- The first part of the decision is broadly relevant to the discussion of surveillance. It concluded that requiring identification is fundamentally reasonable. In other words, the court said that it would balance the modest nature of the intrusion into Gilmore's privacy—required by showing an identification document—against the significant government interest in preventing aviation terrorism. And when it did so, the balance favored the government program.

- The other aspect of the case turned on the notion of consent. The court said that by buying a ticket, when he knew that he would be subject to airport scrutiny, Gilmore had implicitly consented to that scrutiny. The choice to fly on an airplane was Gilmore's, and it was not compelled in any way by the government. And so, the court found, he could not complain about the conditions that the government applied to his choice.

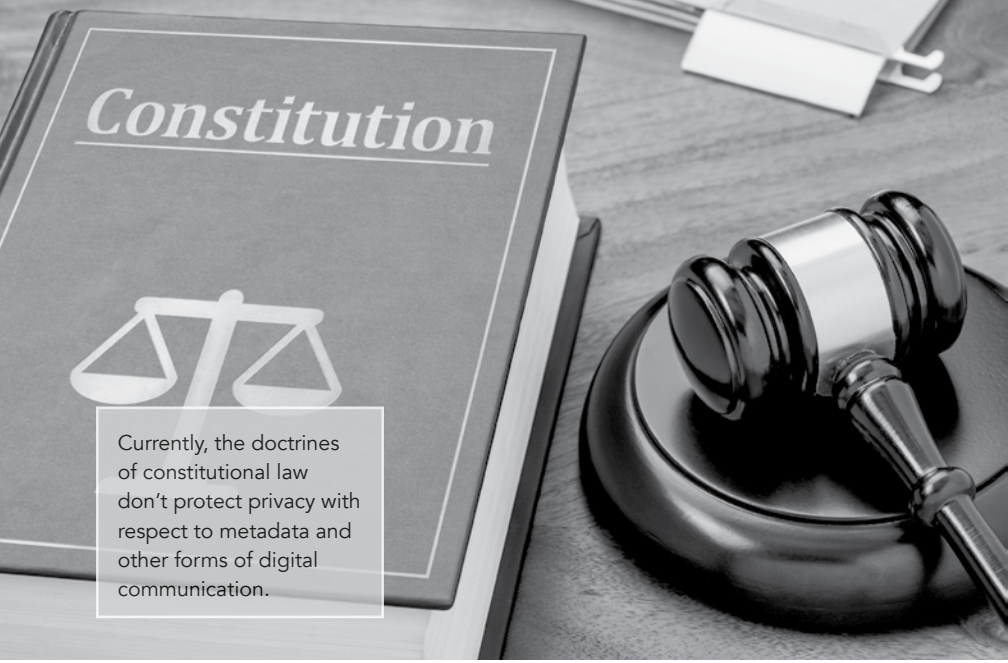
- Gilmore had options in theory—other modes of travel were open to him—but in practice, maybe not. How, other than flying, might one get from Los Angeles to London?

- This idea of consent is relevant to the discussion of the search of metadata. How realistic is it that you won't use a smartphone—and create metadata? The logic of the consent rule in *Gilmore* captures a great deal of everyday life in America today that we would not necessarily think of as voluntary. But there it is—voluntary in theory and mandatory in practice.

The State of Constitutional Law

- The current state of constitutional law is one where the doctrines of law really don't protect privacy—at least not with respect to metadata and other forms of digital information. All of this might change, though, because of growing public and governmental concerns over problems of big data.

- In February 2012, the Supreme Court decided a GPS tracking-related case called *United States v. Jones*, in which four of the nine justices



Currently, the doctrines of constitutional law don't protect privacy with respect to metadata and other forms of digital communication.

(not a majority) said that the collection of large volumes of data raises constitutional issues, because it allows the collection of enough data to create a mosaic picture. With one more vote, the mosaic concern would constitute a majority, and out of that, the court could require government authorities to obtain a warrant to collect bulk quantities of digital data.

- If the court were to go down this path, it certainly would change some aspects of our constitutional law. It would distinguish between the bulk collection of data—such as the metadata in massive databases of calling records—and small-scale collections in individual cases.

- Collecting all metadata might even be prohibited. But when the government sought the metadata of a specific individual, it would be allowed. It is quite possible that the justices will come to recognize that big data collections are different in kind, not just in degree, from collections of small data.

Questions to Consider

1. What would be the consequence if we change the rule about third parties and exposure to the public? How would that affect police practices?
2. How do we define an objectively reasonable scope for the idea of privacy when individual privacy assessments diverge so greatly? Should it be up to Congress? Or the courts?

Your Personal Data Is the Product

Like government spy agencies, commercial data aggregators are involved in a form of surveillance. And some people think that the commercial firms are more of a threat to privacy than the government. What are the risks (and advantages) of commercial data collection and analysis? Does your answer change when it is the government that obtains this private sector commercial data for its own uses? This lecture will explore both issues: the commercial collection of data and how the government uses data that is originally collected for commercial reasons.

Commercial Data Aggregation

- Any consideration of commercial data aggregation should begin with two premises. The first is that *you* are the product. When you click on a link, search the web, or send an email and a company collects data about you, they will be marketing that data to others.

- So, what looks like a free service—Google searching, for example—isn't really free. You are giving Google something of value in exchange: knowledge of who you are. And that, in turn, leads to the second premise: You are getting something of value in return. You get the search service without having to pay for it. So far, it's been a pretty good deal for both parties.

- The Federal Trade Commission (FTC) has recommended that consumer data brokers are to be more transparent and give consumers greater control over their personal information. Former FTC chairwoman Edith Ramirez said, "We need better transparency into how data brokers collect and use our personal information to help ensure that we not go down a path that leads to unfair exclusion, but rather one that widens opportunities for all consumers." This was the start of a campaign to increase government control over data-broker activities.

- At least two results seem certain to follow. First, the growth in regulation of data brokers is part of a broader trend to regulate and control the collection of data generally. The arc of the law and policy is increasingly in favor of regulated data collection, analysis, and use.

- Second, in the consumer context, expect that regulation to rely on something called the principle of responsible use, which is the idea that instead of focusing privacy-protection efforts on anti-collection rules, the appropriate focus is on rules relating to analysis and use.

- The rationale behind the idea is that it is becoming increasingly difficult to place collection limitations on new technologies. As a result, data brokers and cloud storage providers can no longer be effectively regulated through restrictions on their tools of collection.

- That's because collection limitations fundamentally destroy the value of big data aggregation. After all, the whole point of data collection is to discover something new and different. Inevitably, this will mean

that data brokers—and those who store data for the brokers—will be scrutinized for how they use the data they collect.

- We need a flexible conception of responsible use that responds to the context in which data is provided. We assume, for example, that data we provide to an app developer can be used to improve the product we have purchased. By contrast, we have far higher privacy expectations when the data is traded to third parties.

- The FTC's regulation of commercial data brokers is just the beginning. Increasingly, aggregators who collect data from consumers will need to be careful how they use it—because if they aren't careful, they can anticipate a challenge from the government.

The Government's Use of Commercial Data

- It is difficult to measure, but almost everyone is quite sure that the private sector collects—by volume—more data than does the National Security Agency (NSA), or any other government agency. After the 9/11 terror attacks, the intelligence community recognized the value of that data.

- In general, when the government requested assistance after 9/11, commercial providers cooperated, in the interests of national security. Where they were unwilling, the providers were often compelled by law. In time, however, that choice became more uncomfortable for the commercial sector. Often, it now sees cooperation with the government as a public relations burden that it prefers not to bear.

- So, today, Google is encrypting information to avoid NSA scrutiny. Other companies, such as Apple, have limited the amount of data they hold as a way of avoiding the obligation to turn it over to the government.

- Meanwhile, other countries are reacting to American efforts to use commercial data for governmental purposes. The trend globally is toward data-localization requirements—legal obligations imposed by other countries to keep data in the country of origin.

- For example, Brazil is considering whether to require commercial providers to keep data on Brazilians onshore—in Brazil. Russia has demanded that companies like Apple keep data about Russians in Russia.

- Germany has done likewise, and has even banished a large U.S. telecommunications company, Verizon, from competing on German government work—to avoid the possibility that the U.S. government might compel the U.S. company to turn over sensitive information on its foreign ally.

- Government access to commercial data is creating crosscurrents that put companies under competing legal obligations and that are eroding traditional international cooperation.

- The current legal structure creates perverse incentives. Technologically, the most economically efficient place to store data is a product of a number of factors, such as climate, infrastructure, and proximity to users. Law should foster that efficiency, but not at the cost of loss of an individual's or corporation's rights and privileges.

- One bad result would be if some jurisdictions, perhaps out of an authoritarian interests, use legal rule to force companies to store data locally, even though it isn't the cheapest or best place. Another bad result would be a "race to the bottom"—that is, where nations create data rules that are favorable to their own domestic interests while disregarding the globalized nature of the network. In this example, the law could be used as just another type of protectionism.

- A free-for-all of competing nations fighting over commercial data rules serves nobody's long-term interests. But it is a natural consequence of the ad hoc web of domestic laws and international treaties that have grown up in an age of fast-changing technological boundaries. We need to rethink our entire way of approaching the use of commercial data by governments, perhaps even on a global scale. That's an ambitious, perhaps impossible, undertaking. But the alternative is worse.

- Meanwhile, American companies are losing one of their competitive edges because of concerns about government surveillance. That edge is the legal system in which technology innovates and evolves.

- Inconsistent legal obligations put data holders in a nearly untenable position. Although a nation like Germany can demand localization, other nations are not obliged to honor that determination, and many nations' laws conflict with those requirements.

- Indeed, a patchwork of inconsistent laws makes it difficult—though not quite impossible, in some instances—to operate a cloud-based data system.

- According to the Business Software Alliance, a trade group that represents the global software industry before governments and in the international marketplace, legal and regulatory problems—including lack of legal protections and conflicts of law—have substantially impeded cloud-computing growth.

- Consumers outside the United States are losing trust in American tech companies. Anecdotal evidence abounds that American companies are losing business because of perceptions that they are vulnerable to U.S. law-enforcement evidentiary requirements.

- The flip side of this problem is equally troubling. It might be that part of the answer lies in diplomacy. For example, the United States has a mutual legal-assistance treaty with Ireland. That's a treaty that sets out how and when U.S. and Irish law enforcement will cooperate with each other. And it seems likely that the Irish would help American law-enforcement and intelligence agencies—with legitimate interests—to secure the data they need to conduct an investigation.

- But not all nations are as reasonable or as friendly. Some, indeed, are inimical to American interests, and possibly to the interests of many other nations.

- A Chertoff Group white paper noted the following: "The trend toward data localization carries with it the risk that countries might develop rules that make them data-access 'black holes,' where malicious actors can find a safe haven from legitimate scrutiny."

- This is precisely what has happened in other large-scale criminal activities, ranging from the international drug trade to offshore financial centers that facilitated tax evasion and money laundering.

- Sadly, it is unlikely—at least today—that diplomatic cooperation will enable us to chase criminals or economic spies who hide behind the walls of Russian or Chinese law. Thus, at a time when economic pressures—and civil liberties concerns—are driving us to respect the internationalization of commercial data, we also are being forced to come to grips with the lack of a uniform agreement across the globe on what, if any, types of surveillance and scrutiny should be lawful.

- Commercial data collection is of powerful use—both to the commercial enterprise that collects it and to governments that analyze it. But there is no global consensus on how personal and other private data can or should be used, stored, transferred, sold, or safeguarded. Without that consensus, we live, in effect, in a digital Wild West, without law or order.

Questions to Consider

1. Do you use Google? How much would you pay per Google search if it meant that Google was no longer collecting data about you?
2. How do we find a global rule of law to apply to data collection? Is the prospect of American agreement with China and/or Russia on such rules realistic?

The Internet of Things

There are, it seems, an endless number of ways in which information is now collected—new ways that didn't exist 20 years ago. Biometric scanners and facial-recognition cameras are a few of the newer smart devices that we collectively refer to as the "Internet of Things." In this lecture, you'll learn about the proliferation of these devices. Eventually, they will profoundly change how we manage our lives—and create even greater challenges to our privacy and civil liberties.

The Internet of Things

- Tim Sparapani, writing in *Forbes* magazine, postulates that the "Internet of Things" comprises four distinct groupings of enabled products: the Internet of Me, the Internet of Us, the Internet of It, and the Internet of Those.

- The privacy and civil liberties issues surrounding the Internet of Things seem to differ, depending on which type of Internet we are talking about.

The Internet of Me and Us

- The Internet of Me and Us are the Internet devices that collect data on discrete, identifiable individuals. At least three privacy-related questions might be embedded in such collection systems.
  - Who owns (or controls) the data?
  - What are their responsibilities, with respect to protecting that data?
  - What might they be permitted to do with it?

- The ownership/control question is generally established by contract or by statute. Under contract law, the provider of the device almost certainly will claim ownership of the data. As a result, providers generally

consider that they can process the data about the device more or less as they see fit. In that event, however, they also take up the responsibility of providing security for this data about you.

- A Columbia University study found that tens of millions of Hewlett-Packard laser printers were vulnerable to hacking. Even your cloud-based nanny camera could be hacked. Why is that? The manufacturers manage the data they collect in their own best interests, and some of them might not care if your data is used or misused. It doesn't affect them.

- But it seems worth asking a more sophisticated question: Why haven't competitive markets produced more privacy-protective products? Normally, we would expect that if one company treats our data badly, another company will spring up and promise us more privacy and security. Why hasn't that happened yet in the Internet of Things?

- The answer lies in the economics of the industry. Currently, Internet of Things manufacturers might not have sufficient economic incentive to build a better product. In the Internet of Things, personal data is a good—that is, an economic product that can be purchased in the private market. The sale of goods can have benefits for the buyer and the seller. But the sale can also sometimes have effects on third parties that aren't part of the transaction.

- The Internet of Things is rife with third-party effects. Some of them are quite good. When data is collected on energy consumption in your house, for example, it will benefit others on the same network, whose energy efficiency could also be enhanced or who will have more energy available for their own consumption. Indeed, almost every bit of data collected in any part of cyberspace adds to the overall store of knowledge, theoretically lowering the costs of action.

- But the collection of information also can have negative consequences. One is called a diversion effect. If, for example, we collect more information about health, then insurers might choose to only insure the healthy, diverting their actions into more profitable ventures and leaving gaps in the market. A price cut for one might mean price increases for others who are not as well connected or whose business is not so desirable.

- A second negative consequence arises from a pricing problem. We want people who manufacture or market a product to take into account all of the costs of production. But they usually account for only their own costs. How, otherwise, would they calculate a profit? But in the example of a data breach in the new Internet of Things market, the brunt of the cost is likely to fall on the consumer.

- Currently, in general, when software fails to prevent an intrusion—or a service provider fails to interdict a malware attack—there is no obvious mechanism through which to hold the Internet of Things manufacturer responsible for the costs of those failures.

- In a perfect world, you would pay more for your Internet-connected device, and the manufacturer would build better privacy and security into it. In an imperfect world, your device is priced lower, which makes it easier to buy. But consumers experience costs in terms of lost security and privacy.

- What is the solution to this problem? For an answer, let's turn to Ronald Coase, the Nobel Prize–winning economist, and his famous article, "The Problem of Social Cost." His fundamental insights (which quite deservedly go by the name of the Coase theorem) produce an understanding of how the economic reality of harmful third-party effect should, in theory, be linked to legal concepts of duty and liability.

- One of the things that Coase realized is that—in a free market—the person who has the most to gain (or lose) economically will eventually end up paying.

- Coase says that we should expect the parties to negotiate, and whichever one of the two is the beneficiary of the greatest positive net economic value will be the one to actually proceed with their economic activity, while compensating the other party for their forgone opportunities.

- But in the real world, we know that adjudicating liability—or negotiating exchanges of value—takes time and costs money. And we know that information asymmetries sometimes give some actors more or better information than others. We also know that sometimes some of the actors face a collective action problem.

- Taken together, we call these transaction costs—that is, the money that needs to be spent just to make a transaction happen. Sometimes they are small, but sometimes they can be huge.

- This is exactly what we see with respect to the collection of individual data in the Internet of Me. All the little Me's don't have the economic incentive to individually negotiate with Internet of Things providers.

They accept whatever the terms of service are as a condition of getting the new product.

- So, consumers have a collective action problem. Each individual is in a relatively weak position, especially in respect to negotiations with large manufacturers, whose products are the most essential.

- Consumers also suffer from information asymmetries. Internet of Things providers know more about the way their product collects and uses data than do most consumers.

- What is the right economic answer to the liability question in a world where transaction costs exist? The answer (and this is another of Ronald Coase's insights) is to make your best estimate of who the "least-cost avoider" is—in other words, who will incur the least cost to avoid the harm under consideration. If you can correctly identify that person/entity—and allocate the liability there—then you will minimize transaction costs.

- Identifying the least-cost avoider is an empirical problem, and it's a difficult one. It is probably more costly for many thousands of individual purchasers to protect their data and privacy than it is for a manufacturer to build better protections into its device.

- So, Coase tells us that we should write legal rules requiring the manufacturer to protect the data. And that also means that individuals need to be willing to pay a small amount of money to the manufacturer to preserve, and not lose or share, that information.

- But who sets the rules? Who is responsible for figuring out the least-cost avoider? We might do well to try, at least, to solve the collective-action problem through an expression of pure democracy—individuals working collectively, rather than waiting for the government to act for us. It is still a nearly intractable problem. But the good news is that the Internet makes crowdsourcing—a form of collective action—much easier.

The Internet of It and Those

- The Internet of It and Those involve data collection that does not directly reveal our own activities. At least at first glance, those aspects of the Internet of Things seem decidedly less problematic. But they might prove equally disruptive, if not more so.

- Let's say, for example, that your automobile tire tells you that it is low in pressure. What do you do? You fix it, of course. That's the natural reaction. But do you have a duty to fix it? What if you put it off for a day or two and something bad happens?

- Without any recorded information of the problem, you are under a general obligation to make sure that your car is running well. But you would never be found negligent for damage caused by a crash that happened because your tire pressure was low. You just aren't expected to keep track of your tire pressure on a daily basis. It isn't what a "reasonable person" would do.

- How does that change when you start to have perfect knowledge? If your tire tells you that it is low, you might now have an obligation to correct the flaw immediately. And, of course, it isn't just tires. Every component in your car will be reporting to you on a minute-by-minute basis. And that, in turn, might make you legally responsible for keeping your car in tip-top shape.

Questions to Consider

1. What would someone learn about you from a review of the logs of your driverless car? Or of your thermostat?
2. If companies won't protect privacy or security in the Internet of Things for economic reasons, what is the best way to make that happen? Is it civil liability or direct government regulation—or neither?

Anonymity: Going off the Grid

In a world of ever-more pervasive surveillance systems—and decreasing public capacity to control them—it's no wonder that some people want to live off the grid. Around the globe, we have new and innovative ways of capturing information and data, ranging from license-plate readers and closed-circuit television cameras to drones and biometric identification. We are at a precipice, uncertain whether democracy and surveillance can coexist. Faced with this challenge, many people want to simply cloak themselves in the veil of anonymity and become invisible. In this lecture, you'll learn about identity and the anonymity phenomenon.

Identity and Anonymity

- Why is identity important? You might think it isn't. But if you have ever had your identity stolen, you know that who you are and how we identify you are critical to your well-being. The reason for that lies in the idea of attribution: once having established your identity, we can attribute to you corresponding characteristics and responsibilities.

- Today, we tie almost everything to identity. Perhaps more importantly, the idea of attribution lies at the heart of our system for maintaining social order. We want to identify wrongdoers so that they might be punished, thereby deterring bad actors from even considering the possibility of engaging in malicious behavior.

- So, although we sometimes talk about the issue of surveillance as one of privacy, or even liberty, in some ways, government's oversight is essentially tied to identity. Without verifiable identities, we'd have a world of irresponsible actors. But with verified identities, we run into the problem of identity as a means of control.

- The tension between this concept of security and control is palpable. In the United States, mandatory participation in a universal identification

system would be politically unfeasible. You have but to say the phrase "your papers, please" or "national identity card" to evoke a visceral, adverse reaction. In China, by contrast, those types of identification systems are becoming mandatory.

- The American tradition respects, and sometimes even encourages, the ability of citizens to maintain their anonymity as they participate in civil society. Anonymous and pseudonymous speech has a long history in the United States.

- The case for anonymity is that it facilitates the expression of unpopular views. On the other hand, anonymity can be a cloak for malicious speech. The balance is not ineluctably set in either direction.

- The Supreme Court was called upon to resolve the conflict. Relying on American history—and on the values underlying the marketplace of ideas—the court recognized a First Amendment right to anonymous political speech.

- Many see the Supreme Court's decision as stating a broader principle that, in general, the judiciary will disfavor a legislated identity requirement. That can't be an absolute, of course; we didn't just outlaw driver's licenses. But it does mean that there is, at the core of American society, a respect for privacy in the form of anonymity.

- Some aspects of newer technology support that fundamental attribute of American life, as does some of the cultural history of its development. Attribution on the Internet is one of the network's more alluring and elusive technical aspects.

- Network protocols do not, at their core, require identification. So, connectivity comes with the background assumption that anonymity will be allowed. That makes it technically difficult, though not impossible, to identify those on the network who wish to remain anonymous.

- Ben Wittes and Jodie Liu, writing for the Brookings Institution, found that many aspects of technology support privacy in interesting ways. In fact, web browsing can enhance one's privacy.

- The other pillar of anonymity is cultural. Anonymity on the Internet stems not just from the architecture of the communications protocols; it also reflects the quasi-libertarian streak at the core of early Internet society.

- For some of the original designers of the Internet, anonymity was a way of giving individuals greater power to resist or avoid the government—a view to which they had an ideological commitment independent of their technical work. Consequently, even as technology labors to deliver more and more connectivity, some of the architects of this connectivity also build in security and anonymity frameworks.

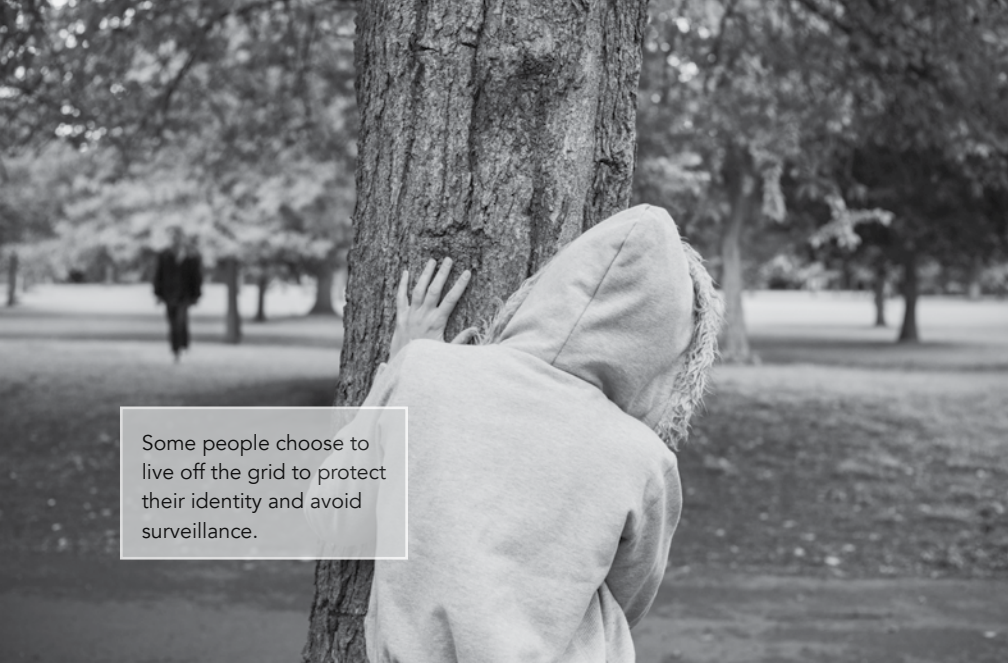
Trying to Find a Balance

- The growing use of biometrics is the one technology that poses the greatest challenge to traditional concepts of anonymity. Put more affirmatively, biometrics—by definition—is a means to decisively and irrevocably fix physical identity.

- That's why some civil libertarians and privacy advocates oppose almost all forms of biometrics. They believe that liberty derives from anonymity. Supporters of biometrics, pressing the alternative view, are of the belief that proper security is dependent on identification.

- Perhaps instead of depending solely on anonymity or full identification, Americans would be better served by a range of authentication solutions—variable ways in which identity might be determined, in whole or in part. The following are some things to consider.

- Anonymous political speech remains an important ideal for maintaining liberty. But outside of this specific realm, anonymity is a different, and possibly weaker, form of liberty.



Some people choose to live off the grid to protect their identity and avoid surveillance.

- The American understanding of liberty interests necessarily acknowledges that the identity of those who have not committed any criminal offense can be collected for legitimate governmental purposes through biometrics. You must, for example, allow a photograph to be taken for your driver's license.

- On the other hand, liberty could be put at risk if identifying biometrics were required for even the smallest interaction with the government, such as using a government public web site.

- So, we want to start asking whether between complete anonymity and full identity we can develop gradations appropriate to select circumstances. Many interactions with the government or other people can be accomplished without requiring detailed personal information, though they would not be completely anonymous.

- Indeed, we already have the beginning of a graduated understanding of identification; sometimes identity is only needed to authenticate

something—that the transaction is what it purports to be. In that context, identity is not essential. The credit card transaction needs to know that money is available, but in most cases, who is paying is not critical information.

- In other contexts, you must know whom (or what) you are dealing with. Thus, there is a spectrum of authentication—and personal identification—solutions available to the government.

- Consider a transaction where no identifying information about the individual is necessary, but actual authentication is needed. This might be the circumstance when, for example, data is going to be used in an ongoing government research study.

- Contrast that with the situation where the actual identity is not important, but identifying information is necessary. For example, in regulatory documents filed electronically by a company, who files is not important, as long as we can be sure that it is the company that is filing.

- These examples demonstrate that our conceptions of identity are based not on absolute privacy expectations, but rather that any government infringement on our liberty will occur only with good cause.

- The right policy will allow citizens to voice controversial political viewpoints with the expectation that the government will investigate only those who truly might threaten national interests. When a criminal or terror investigation is underway, we must be able to expect that the spotlight of scrutiny will not turn on us individually—without some good reason.

- Most interactions with the government fall somewhere in between expectations of complete anonymity and a detailed investigation. We must be able to continue to expect that the government will ensure that any possible impingement on liberty is commensurate to the interaction with the individual and that the government has the technological tools to achieve this.

- If there is no true spectrum of authentication choices (from anonymity to pseudonymity to full identity), all expectations of privacy will erode, because government will be forced to treat every interaction as investigative.

- In many ways, the implementation of new laws and systems to enhance surveillance are not universally anti-privacy and anti-liberty. Rather, new laws and practices can substitute one privacy intrusion (for example, the search of electronic biometric data about an individual) for another privacy intrusion (the physical intrusiveness of body searches before entering an airport or courtroom). But this means that legal analysts cannot make absolute value judgments.

- Each person weighs the utility of his or her own privacy by a different metric. For many Americans, the cost to liberty of a little less anonymity might not be too great, if it results in a little more physical privacy, in certain circumstances. For others, the opposite result might be their choice.

- Reasonable people can disagree about when identification technology should be used. But taking a position that any use of biometric identification technology is anonymity destroying and privacy invasive ignores the positive benefits that this surest form of identification presents.

- It's not just that your DNA, iris, or fingerprint are sometimes the surest proof of your innocence when wrongly suspected of a crime; they are also the greatest potential gatekeepers of your genetic legacy and, therefore, of other privileges, such as security clearances and family identification.

- The true policy challenge is in finding the most effective uses of the identification technology for liberty and security—not in labeling any of them as universally good or evil.

Questions to Consider

1. Think of cases where you value your anonymity. Now think of times when you absolutely need to know who you are dealing with. What distinguishes those situations in your mind? Is it only about what is best for you in that particular situation, or are their common themes on which we can draw?
2. Governments say, in effect, that the use of anonymizing technology is, by itself, an indication of the need for additional scrutiny. Are they right as an empirical matter? And if they are, does that mean that they are right as a matter of policy?

Code Breaking versus Code Making

To avoid surveillance, some people turn to encryption. They code their communications into undecipherable gibberish to hide it from government scrutiny. But they aren't always successful. In this lecture, you'll learn about how encryption works and why it is important. In addition, you'll discover some of the legal and policy issues at the intersection of surveillance and civil liberties that surround encryption, making it a complicated issue for the government, service providers, and individuals.

How Encryption Works

- Edward Snowden's unauthorized disclosures of state secrets, and the related fallout, brought the encryption issue to the forefront of the surveillance debate. Many major providers of mobile-phone operating systems—including Apple, Google, and Microsoft—announced that they would offer new products that automatically enabled the encryption function and that they would not keep any encryption keys.

- Now, the only person who could unlock an encrypted phone would be the owner. In turn, the U.S. government expressed great concern that anti-terrorism efforts would be compromised. The FBI director himself came out in direct opposition to the plan.

- Encryption as a defensive mechanism is not a perfect solution. But what it can do is ensure that your information is confidential and can't be read by anyone else without your permission.

- Modern algorithms also can provide you with a means of confirming that the information has not been tampered with in any way. Advances in cryptographic technology have made it increasingly difficult for individuals to crack a code.

- Naturally, code breaking is as old as code making. But encryption increasingly has advanced beyond decryption to the point where decryption, in some cases, is almost impossible.

- This has the positive benefit of enabling legitimate users to protect their lawful secrets. But if the United States government—or Syrian activists—can encrypt their data, so, then, can China, or the Russian mob, or a Mexican drug cartel.

- This brings us to a series of tough questions: Should a government require the manufacturers of encryption technology to limit their distribution to prevent strong cryptography from falling into malevolent

hands? Should the state, in effect, be able to require that code makers build in a "backdoor," by which authorities can access and decrypt encrypted messages? And under what rules might these backdoors be accessed?

- Conceptually, encryption involves three separate components: the plaintext, the algorithm, and the key. The plaintext is the substance of the message that the sender wants to convey. This information doesn't have to be text; it can be any data in any form that is more valuable to the sender if kept unknown to someone else.

- The algorithm is a general system of encryption. In other words, it is a general set of rules for transforming a plaintext. An example of an algorithm is a cipher where, for example, each letter of the plaintext might be replaced with another letter. The algorithm here is "replace each letter with another."

- The third, and most essential, component of an encryption system is the key, which is the specific set of instructions that will be used to apply the algorithm to a particular message. A cipher key might be to "replace the original letter with the letter that is five letters after it in the English alphabet."

- Using this simple algorithm and key, the plaintext "cat" could then be converted into the gibberish "hfy," and the result would now be known as the ciphertext.

- The critical feature is that only someone who has the algorithm and the key can decrypt the ciphertext. So, even if the ciphertext is physically intercepted, the contents remain confidential.

- We've been creating ciphertexts for quite a long time. Julius Caesar's use of codes was so common that the type of algorithm he used—the letter-shift system just mentioned—is sometimes called the Caesar cipher.

Encryption and Decryption

- It is a fair assessment of the art of cryptography that until the dawn of the computer era, decryption was quite effective. The keys themselves could be stolen, or they could be decrypted. These things stood for a number of years. Those who wanted to keep secrets were vulnerable.

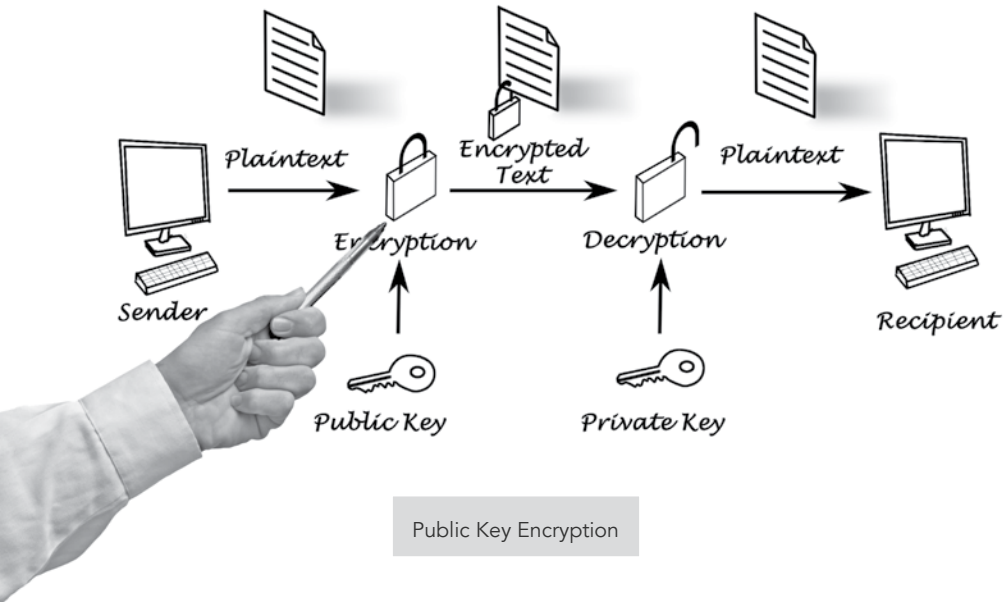
- In the late 1970s, however, enterprising cryptographers developed a way to encrypt information using the multiplication of two extremely large prime numbers and certain one-way mathematical functions.

- Most mathematical functions, such as addition and subtraction, work in both directions. You can get the results from the precursors, or you can get the precursors from the results.

- In contrast, a one-way function works in one direction. With one-way functions, someone who wants to receive encrypted messages can publish the result of an extremely large multiplication as a public key. People who want to send this person a message can use the public key to encrypt their message. And because only the creator knows how to break down his or her exceedingly large number to its original primes, only he or she can decrypt the message.

- Today, you can embed this type of encryption into your email system with an expensive software program. If the users at both ends of a message use this form of public key encryption, the message they exchange between themselves becomes, effectively, unbreakable by anyone other than the key's creator—unless, of course, a hacker attacks the creation of the key at its source.

- The United States prefers not to hack American companies in this way, if it can avoid it. The government's preferred solution is as follows: Those who manufacture encryption software should build into the system a backdoor decryption key that will allow the government to read any encrypted messages.



Public Key Encryption

- The decryption keys would be stored (or escrowed) with a trusted third party (for example, a judge at a federal court), who would release the key under only specified, limited circumstances. Many privacy advocates oppose the effort, and their opposition has been successful so far.

- In the 1990s, the FBI sought to require encryption-technology manufacturers to incorporate a backdoor named Clipper Chip. Opposition to this was based in part on civil liberties objections. Many people were concerned that the backdoor would be used for political purposes, rather than to combat crime. The opposition was also based on a practical realization that the government was a beneficiary of strong encryption to protect state secrets.

- A backdoor in encryption programs would not necessarily be available only to the U.S. government, after all. The United States has no monopoly on the development of encryption algorithms. If the United States required backdoors in American products, purchasers abroad would naturally tend to favor non-American products. So, the state would primarily have a backdoor into its own secrets.

- Until recently, the balance still favored the government—because companies would often hold master encryption keys to their customers' data. They might do so as a convenience. If you encrypt your data and then forget or lose your uncrackable encryption key, then the data is lost forever. So, you might be very glad if your phone provider could unlock your phone and let you recover all of your data.

- Because strong encryption is, for most purposes, uncrackable, governments have turned to an alternate method of securing access to encrypted communications—that is, forcing those who do the encryption to provide it with the encryption keys to decrypt the messages directly. As a result, governments are bringing increasing pressure on service providers to turn over their master encryption keys.

Legal and Policy Issues

- Sometimes the endpoint user—the individual—holds the encryption key, and sometimes the user's service provider does. Who has it makes a world of legal difference. When the encryption key is held by your service provider, it is likely that the government can get access to the passwords.

- When you hold it—and when only you hold the key—it is much more difficult for the government to get access. And that is why the move toward automatic endpoint encryption—by Google, Apple, and Microsoft, among others—is so significant for privacy and civil liberties.

- The Fifth Amendment says that we all have a constitutional right to withhold from the government testimonial evidence that might be used to convict us of crimes. It is sometimes called the privilege against self-incrimination.

- Service providers like Google and Microsoft might resist the government's pressure—and they would be wise to do so for business reasons—but in the end, they will not succeed. By contrast, the individual, who holds his or her own encryption key, has a much stronger

argument to withhold it under the Fifth Amendment protection against self-incrimination.

- The courts have yet to definitively determine whether or not an effort to compel that individual to disclose the decryption key constitutes a violation of his or her Fifth Amendment privilege. But the trend is in favor of the individual's protection.

- In general, the answer to the question turns on whether disclosing the decryption key is thought of more like the production of a physical object (such as the physical key to a lock box), which might be compelled, or like the production of a person's mental conceptions (such as the memorized combination to a safe), whose disclosure cannot be forced.

- The issues raised by the government's push for greater decryption authority reflect policy questions more than they do legal ones. For example, what would be the security implications of requiring decryption capabilities in new technologies? How would granting the U.S. government the access it wants affect international perceptions of American conduct?

- With respect to security implications, building in decryption capabilities would necessarily introduce potential vulnerabilities that could be exploited—not by those who would have authorized access, but rather by hackers who might find a way to crack the capabilities of the protection itself.

- With respect to granting greater decryption capabilities to governments, it is difficult, if not impossible, for the United States to oppose such efforts in international forums when its own policy favors expansions of interception and decryption capabilities domestically.

- However, U.S. policy also advocates Internet freedom, in large part as a way of energizing democracy movements around the world. And that policy is difficult to square with a domestic move toward greater governmental decryption capabilities. After all, what the U.S.

government wants might be exactly what China or Russia want as well. Is that really the company we want to keep?

Questions to Consider

1. Should you have the privilege not to tell your passphrase to the government? If you think that the answer is yes, why is that different from your fingerprint or blood? Does the physical/mental distinction make sense?
2. What would you think if you were assured by security experts that a "government-only" backdoor could be created? Would you accept it, provided that it was opened only with a court order, or would you think it was too intrusive? Why?

Europe's Right to Be Forgotten

In discussions of surveillance, civil liberty, and privacy, many of us often limit ourselves to American concepts of law and liberty, the American experience of spying by U.S. intelligence agencies, and commercial surveillance by American companies. But the American approach to these issues is not universal. And as you'll learn in this lecture on European views, America is something of an outlier on these issues compared with other Western nations. That being said, the West generally is aligned on the concepts of privacy, civil liberties, and autonomy—values that we all honor, albeit in different ways.

European Privacy

- For Europeans, privacy is a right. For Americans, it probably isn't. The right to privacy in Europe is considered so fundamental that it is enshrined in the European Charter of Fundamental Rights. Article 8 states, "Everyone has the right to the protection of personal data concerning him or her."

- The basic rules underlying privacy rights for members of the European Union are set forth in a pan-European rule known as the European Union Data Protection Directive. That directive controls how European companies can process personal data.

- The directive applies to electronic filing systems, and old-fashioned paper ones. The data covered by the directive is information about an individual that somehow identifies a person by name or otherwise. It's what we call personally identifiable information.

- One oddity is that these pan-European directives are not self-executing. Instead, they are treated as a baseline of guidance for each member state. Then, each national government is responsible for implementing the directive.

- There is a fair bit of variation between, for example, Germany and Greece. But the directive serves as the core guiding principle. And since it was adopted in 1995, every country in the European Union has implemented it.

- The directive begins by laying down basic privacy principles. They are derived from a set of internationally recognized practices for addressing information about individuals known as Fair Information Practices. They essentially codify the requirement that information should be collected for specific, legitimate purposes only and stored in individually identifiable form no longer than necessary.

- The European directive also states that the person whom the information is about has some rights of his or her own. In particular, a company collecting such information must give the person notice explaining everything about the data collection. That is, the person who is subject to this information sweep is entitled to know who is collecting the data and why it is being collected—as well as who will have access to it.

- There is also a transparency requirement so that the person can have access to the collected information and correct it, if needed.

- There is, however, one gaping hole in the data directive. It doesn't apply to participating European governments. The member states exempted themselves from the directive to the extent that it might apply to many of the state's own operations.

- So, for example, the directive's requirements don't apply to matters of taxation, criminal matters, or matters of national security. The European Parliament has considered revisions to the data directive that would, at least partially, close that loophole. But national governments have stood in opposition.

European Privacy in the Commercial Sphere

- In the United States, the two principal—and competing—ways of protecting privacy have been to restrict collection and restrict processing. In other words, we sometimes protect privacy and civil liberties by saying the following to a company: This is data you may not collect in the first instance.

- The other limit is on processing, or what is sometimes called "use": the idea that you can collect the data all you want but use it only for the specific purpose that you collected it for—or, perhaps, that you can use it for another purpose but only with permission from a court, a supervisor, or some other authority.

- The European model has one other, different way of protecting privacy. It allows people who feel that their privacy has been infringed upon to request—and require—that even truthful information about them be deleted or obscured. The Europeans call this the right to be forgotten.

- For many years, this concept was discussed and argued about on the other side of the Atlantic. The U.K., for example, generally holds that after some unspecified period of time, criminal convictions can be "spent," or exhausted, on the expectation that the offenders have been rehabilitated—such that the prior criminal acts shouldn't be relevant, for example, to employment. France has adopted a similar view, called the right to oblivion.

- But this right to be forgotten didn't come to prominence until May 2014, when the European Court of Justice—Europe's highest judicial body—considered a case brought by a Spanish man named Mario Costeja González.

- In 1998, Mr. Costeja Gonzalez had his foreclosed home sold at auction. He later paid that debt, but the fact that he had been a debtor was recorded for posterity in a digitized 1998 article in the newspaper *La Vanguardia*.

Unlike for Americans, privacy is a right for Europeans.

- Mr. Costeja Gonzalez originally complained to the local Spanish Data Protection Agency, asking for the article to be removed from the web. But the agency rejected his complaint on the grounds that the newspaper article was lawful and accurate.

- The authority did, however, accept a complaint against Google—and asked the U.S. company to remove links to the article from the search results that were derived for Mr. Costeja Gonzalez's name, even though Google wasn't the author of the article.

- The argument was that the search engine was at fault because it made the article visible to a large audience. Rather than just delete links to the offending article, Google sued the Data Authority in Spanish court. And that national court, in turn, referred some of the questions before it to the European Court of Justice, which ruled that search engines are responsible for the content they point to.

- Thus, Google was required to comply with European Union data privacy laws. And that, in turn, means that individuals can ask Internet search sites to remove links to web pages that contain "inadequate, irrelevant or no longer relevant" information in the results page for searches of their names.

- Since that ruling, Google has requests to remove more than nearly 300,000 links and has removed 40 percent of those requested. And that number grows each day.

- So, there is sometimes a warning at the bottom of the U.K. page (www.google.co.uk): "Some results may have been removed under data protection law in Europe." That's Google's way of letting you know that the subject of your search might have asked for his or her name to have been removed from an old link.

European Government Surveillance

- With regard to how European views differ with regard to privacy and government surveillance, one perception is that Europeans are much less tolerant of government surveillance than Americans are. The massive, unauthorized data disclosures by the former National Security Agency (NSA) subcontractor Edward Snowden—revealing some of the hidden practices of American spycraft and diplomatic relations—seem to have only reinforced the uneasiness of Europeans (and others) with the idea of American surveillance.

- A common reaction across Europe was to publicly call for suspending intelligence-sharing agreements that cross the Atlantic. In truth, however, many observers think that the European reaction was quite muted in practice. One would be hard-pressed to find any trans-Atlantic cooperation that was actually suspended.

- We want the world order to aspire to high-minded values, and we want the United States to interact with international institutions, such as the United Nations and the World Trade Organization, on the basis of those higher ideals. U.S. sponsorship of such ideals and institutions

contributes to their legitimacy. But in its national capacity, the United States doesn't always practice what it preaches.

- Another indication that there is less space between the United States and its allies than perhaps meets the eye is in the reaction that various nations had to the Snowden disclosures.

- After the *Charlie Hebdo* massacre in France—during which two militant brothers forced their way into the offices of a satirical newspaper and killed 12 people—the French assembly overwhelmingly approved legislation that gave authorities their most intrusive domestic spying abilities ever—with almost no judicial oversight.

- The law gave French officials the right to tap cell phones, read emails, and force Internet providers to comply with government requests to sift through virtually all of their subscribers' communications.

- Among the types of surveillance that the French intelligence services were authorized to carry out was the bulk collection (and analysis) of metadata, similar to that which has been performed by the NSA.

- The French intelligence services could also request a right to put tiny microphones in a room or on objects—such as cars or in computers—or place antennas to capture telephone conversations or mechanisms that capture text messages. French citizens and foreigners alike could be tapped.

- At almost the same time that the French were moving to expand government surveillance powers, a controversy erupted in Germany. It appeared that the German intelligence agency, known as BND, had been helping the NSA by conducting electronic surveillance and data analysis of other European countries, most particularly the French.

- Needless to say, the French were none too pleased to learn this. And because the German cooperation with the United States appeared

to contradict earlier German protestations against NSA surveillance, charges of hypocrisy flew.

- The real question is not whether privacy is better protected in Europe. Europe does have more comprehensive consumer privacy rules than the United States, but those seem inapplicable to the government surveillance question.

- Nor is the real question whether or not government surveillance occurs less in Europe. As to that issue, Europe and the United States are converging rather than diverging. At least the French example suggests that is the case.

- So, the question we might want to ask is as follows: How does American intelligence oversight stack up next to European intelligence oversight? If this is the question, U.S. law and oversight of its intelligence agencies is (perhaps surprisingly) more robust—not less—compared with Europe. Judicial limitations are more stringent in the United States, and transparency is greater, too.

Questions to Consider

1. What accounts for the differences in European perspectives? Is it history? Culture? Something else?
2. Do you think the differences between America and Europe are significant? Are the gaps bridgeable or irreconcilable? Is the First Amendment an insurmountable stumbling block to agreement?

National Security and the First Amendment

Court cases involving the news media provide a host of interesting questions concerning policy and law, not all of which come with satisfactory answers. There are three questions to consider in this lecture: What is the proper role of the news media in covering government intelligence-collection and surveillance activities? How should the government respond to press coverage of intelligence collection—with tolerance or with criminal prosecution? Who is a journalist?

Expectations of the News Media

- In America, we have a longstanding ideal that advocates for the freedom of the press. The right is enshrined in the First Amendment to the Constitution. In landmark litigation from an earlier era, including the famous Pentagon Papers case, we developed a series of rules that favor allowing the news media to publish classified information.

- A traditional view has been to regard the news media as a watchdog, ferreting out wrongdoing. But why is that? What is it that we expect journalists to do? Is it simply a means of insuring transparency of what the government does? Or do we think that this extended privilege has a more limited (but perhaps more important) role to aid in checking malfeasance, misfeasance, and nonfeasance by government officials?

- A fair assessment is that the role of the news media is changing before our very eyes. Several cases reflect the changing norms of reporting on national security. But the balance seems to be shifting toward greater transparency.

- How should the U.S. government react to these changing norms? Although President Barack Obama expressed a desire for balance, his administration made significant efforts to prosecute leakers (as a way of deterring leaks). Indeed, it is fair to say that the Obama administration

has been more aggressive than prior administrations, having brought at least seven such prosecutions during the President's term of office. Among those indicted recently are familiar names: Chelsea (formerly Bradley) Manning, who was convicted, and Edward Snowden and Julian Assange, both of whom have yet to be tried.

- On the whole, the government has significant power to prosecute leakers—a power that it has used less than a dozen times in the last 50 years. Despite this power, journalists have historically been treated differently from the leakers themselves. Journalists have gone to jail for not disclosing sources and have been threatened with prosecution, but there never has been a case where the U.S. government actually prosecuted a journalist for receiving and publishing classified

information, even though the Constitution—and the law—would seem to permit that.

- In 1971, in the Pentagon Papers case (*New York Times Co. v. United States*), the newspaper published a confidential report of how the United States became involved in and conducted the Vietnam War.

- The court refused to halt publication—something called prior restraint. The court said that the government failed to show that publishing the report would cause "direct, immediate and irreparable damage to the nation or its people," and it allowed *The Times* to proceed.

- But in an ominous aside, Justice Byron White (who would have allowed the prior restraint) noted that news media might be held criminally liable after publication for disclosure of sensitive national secrets.

- Nonetheless, only once in its nearly 100-year history has the Espionage Act been used to prosecute a third-party recipient of national defense information, as opposed to the government employee who disclosed it. That was in the 2005 indictment of two lobbyists for the American Israel Public Affairs Committee (AIPAC) for facilitating a State Department employee's leaking of national security secrets to Israel. That prosecution was abandoned after a U.S. district court, motivated largely by First Amendment concerns, imposed a heavy evidentiary burden on the government in pretrial rulings.

The News Media and the Law

- Past conflicts between the government and the news media have not converged in criminal prosecutions; rather, they have emerged in the efforts of government investigators to expose the news media's confidential sources in leaks of national security and other sensitive information.

- To do so, the government has relied on the common-law precept that "the public has a right to every man's evidence" (except for those protected by a constitutional, common-law, or statutory privilege). And

it has argued that the press has no privilege and might even be liable for publishing state secrets.

- Justice Byron White again helped define the legal landscape when he wrote the majority opinion in a 1972 case called *Branzburg v. Hayes*, in which the question was whether or not the First Amendment right to publish carried with it a constitutional right to promise confidentiality to sources.

- The court rejected that idea. As Justice White said, journalists were asking the court to set out "a testimonial privilege that other citizens do not enjoy" and that while not being able to protect a source's identity might crimp the news-gathering process, "from the beginning of the country the press has operated without constitutional protection for press informants, and the press has flourished."

- Still, all was not lost for the news media. In his dissent, Justice Potter Stewart argued that in seeking a subpoena to compel a journalist to testify, the government must "convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest." Even though his opinion wasn't controlling law, it has, over time, become the legal norm.

- Efforts to enact a statutory standard for whether—and when—the Justice Department will use its subpoena power to collect electronic records from the news media have, so far, failed in Congress. For now, however, the only thing that limits federal surveillance of the news media is its own self-restraint.

- Under a great deal of public pressure after the case involving a national security reporter and a State Department contractor during the War on Terror, the Justice Department adopted a new policy. In summary, this policy makes clear that the government will "provide protection to members of the news media from certain law-enforcement tools, whether criminal or civil, that might unreasonably impair ordinary newsgathering activities."

- It says that subpoenas and search warrants directed at members of the news media are "extraordinary measures, not standard investigatory practices" and must be authorized by the attorney general. In criminal cases, the information sought by the government must be essential to a successful investigation or prosecution, and prosecutors must make "all reasonable attempts" to obtain the information from alternative, non-media sources.

- All of that sounds good, but because the attorney general issues the guidelines and interprets them, it means that the president's chief legal officer is judge and jury when it comes to the appropriateness of news media scrutiny.

- This tension—between prosecuting leaks of classified information and providing for at least some nominal public window into national security activity—reprises the larger question: Can security and civil liberty coexist? Can democracy coincide with secrecy? The two, it seems, are in a never-ending tension that can't quite be resolved in any categorical way. We seem to have to treat each case individually as they come up.

The Nontraditional News Media

- In some ways, the nontraditional press, epitomized by the likes of Julian Assange and WikiLeaks, is not terribly different from traditional media. It reveals, and sometimes comments on, previously nonpublic information. But such practitioners might also be more adversarial, more partisan, and more slanted. Consequently, they might also be less likely to exercise restraint and more likely to pursue transparency as an absolute value.

- If you see the development of greater surveillance methods and technologies as strengthening the hand of government intrusion and abuse, it's likely that you will welcome the transparency advocates. If you fear the threat to national security they might pose, you will not.

- Serious journalists and policy professionals understand the challenge. They give the competing values purposeful consideration and do their best to manage the issues on a case-by-case basis. There is a high-

Julian Assange (1971–), Australian computer programmer and founder of WikiLeaks

mindedness to the serious journalist's efforts that deserves our respect and support. But sometimes, the news media misses the mark and errs on the side of transparency.

- The journalist and constitutional lawyer Glenn Greenwald helped the U.K. newspaper *The Guardian* win a Pulitzer Prize for public service based on his reporting about the National Security Agency—which stemmed in part from the Snowden leaks. Greenwald went on to cofound the digital news imprint known as *The Intercept*.

- Consider a report by *The Intercept* that chose to disclose a security vulnerability of the U.S. Transportation Security Administration (TSA). In particular, the digital news publication reported that the TSA had sent its staff a notice about a type of explosive that the agency's security filters were not equipped to detect. To be clear, there is no allegation of misconduct, malfeasance, or error here.

- The closest *The Intercept* could come to formulating a justification for publishing the classified material—the revelation of which could endanger the traveling public—was that there was a bureaucratic "CYA-type" nature to disclosure.

- In other words, the TSA had a problem for which it didn't have a technological solution and wasn't likely to in the near future—which meant that we were at risk. At a minimum, the TSA wanted everyone to know that it knew so that if something went wrong, it wouldn't be charged with incompetence, just technical inadequacy.

- Is bureaucratic gridlock a ground for disclosing information that could result in real harm to individuals? The moral calculus underlying that argument is questionable.

- There are any number of reasons to think that the TSA is not doing a great job, but identifying and alerting staff to a vulnerability for which the agency had yet to devise a solution reflects good governance. It is not an example of incompetence or misfeasance.

- So, why would *The Intercept* publish such a piece? Transparency, without oversight—or audit, or review—is nothing more than voyeurism. At bottom, that reflects moral vacuity. It is a failure to grapple with the difficult questions of justification and need. These justifying values are replaced with little more than narcissism.

Questions to Consider

1. The press has a special place in America. Do you think that means that journalists should have special rules as well, or would exempting them give them too much power?
2. If the recent upturn of prosecutions of leakers is intended to stop the flow of leaks, it doesn't seem to be working. Why not?

The Privacy Debate Needs You

This course is not aimed at resolving the fundamental tensions that exist permanently in American democracy. It's about managing them, living with them, and accommodating the competing values to the maximum extent practicable. The discussion—and the tensions—you've learned about in this course are emblematic of the value of competing ideas; they reflect a living, breathing aspect of a functioning democracy. In the realm of policy and law, we continually attempt to square the circle of security and liberty, never succeeding and, quite possibly, never really expecting that we can succeed. Rather, this unending tension calls for us to continually rebalance and reexamine fundamental values, trying our best to give effect to both as circumstances permit.

The Human-Computer Interface

- It blows one's mind to learn that the U.S. Army is working to develop drones that can be deployed and controlled by human thought. Nonetheless, that's the case. Scientists at the University of Texas at San Antonio got a grant from the military to do just that.

- It's been reported that the researchers got one grant from the Office of the Secretary of Defense for 300,000 dollars to investigate the possibility of military personnel using brain signals to operate drones for surveillance, intelligence, and reconnaissance missions.

- This came with a companion Pentagon grant of 400,000 dollars that allowed the University of Texas to buy two top-of-the-line electroencephalogram (EEG) systems—systems that are designed to measure and report out brain waves.

- The plan is to start small with very small drones, such as those employed by hobbyists. The long-term goal—which might never be realized—is to

have soldiers flying large military drones via thought control, navigating with the power of their own minds.

- Interestingly, a development like this might not require much change in our thinking about law and policy. After all, whatever the legal rules are that we develop to govern drone use and airspace rights, what difference will it make if they are flown by brainpower?

- In one sense, the difference really won't matter. But in other ways, small increases in technological capability and ease of utility tend to transform themselves into larger disruptions of settled expectations.

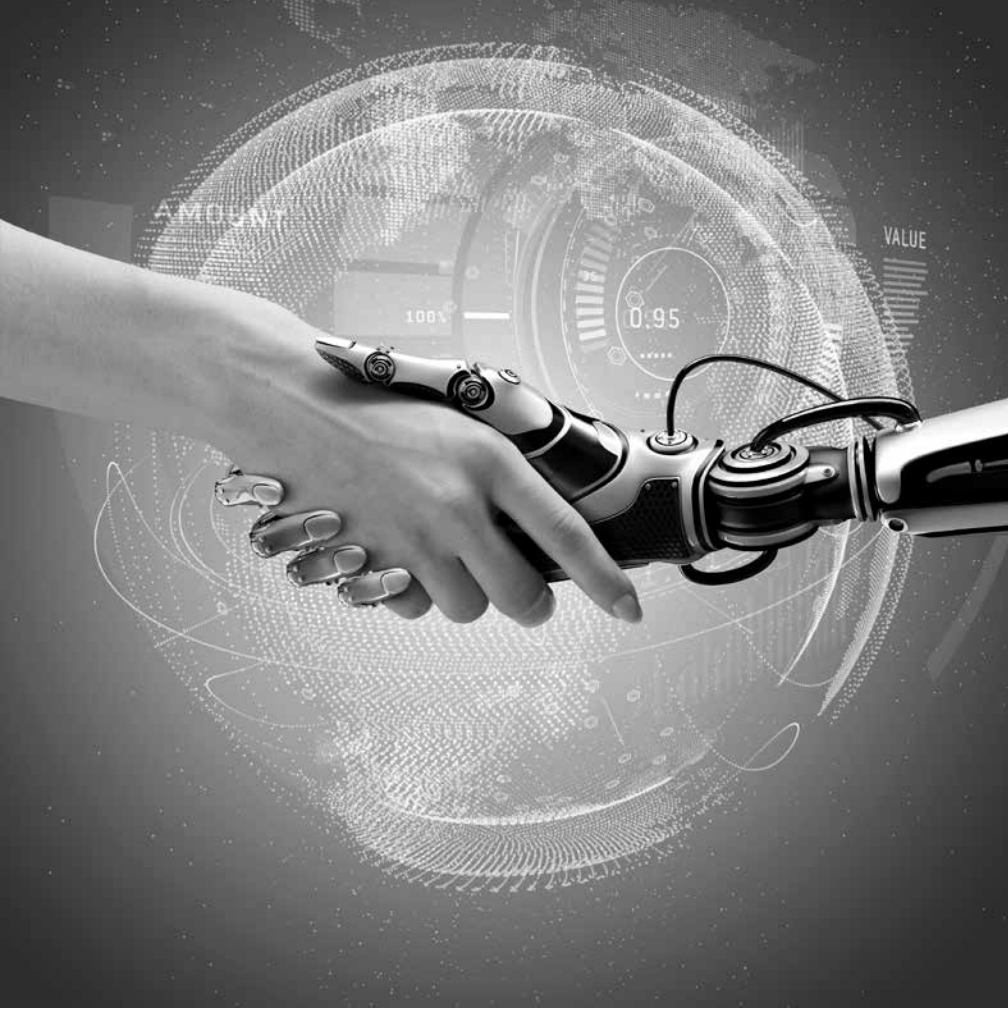
- Mind-controlled technology will—or might—offer technological ease-of-use so great that it ends up making a real difference in law and policy.

- Instead of having to carry a controller, or computer, to operate a drone, we can imagine that soldiers will one day have EEG sensors in their helmets so that they can direct attack and surveillance drones. A military scout could, for example, control a drone and have it fly over an adjacent ridge, sending back pictures of the enemy's position to his or her headset. Likewise, a police officer equipped with a mind-controlled drone could quickly and readily get a tactical picture of a hostage situation. This potential ease of use would also present grave risks of misuse.

Artificial Intelligence

- Let's turn to artificial intelligence, or what many prefer to call autonomous learning machines. An important distinction lies in the word "learning." There are many autonomous machines in existence already, such as robots on assembly lines. While these semiautonomous machines can operate independent of human control (hence the autonomous part of the name) they are not, generally, adaptive. They don't learn from experience; they don't adapt to unanticipated situations. They only do what they are programmed to do.

- Learning machines are different. They can adapt. They can learn from success or failure. They soon might be able to build a mathematical



model of a future choice, make predictive judgments based on that model, and then evaluate the result and modify the model. In short, they are programmed to be capable of doing things that are unexpected and unanticipated.

- They might not have "souls," so we won't call them "alive," according to traditional meaning. But they are something else that is very important. They are surprising.

- Consider, for example, the programming required to operate a driverless car. It has to adapt, in the same way a human driver might, to situations that it hasn't seen before. It turns out that many of the best-performing driverless vehicle algorithms share a common trait: humans have not explicitly programmed them.

- What is true of weapons systems seems to be equally true of any autonomous learning machine with surveillance capability. It is a real risk to society if we remove the element of human control from our machines.

- Some of the greatest thinkers of our time, such as Stephen Hawking, Bill Gates, and Elon Musk, all share similar concerns. They worry that artificial intelligence is a grave threat to humanity. They might or might not be right, but it certainly seems that the surveillance, data collection, and analytical capabilities you've learned about in this course are, in effect, a force multiplier. Even under human control, such powerful systems shift the balance of authority toward those who control them. That's what generates such a significant counterreaction from the public.

- One does not need to be a Luddite—or an apocalyptic visionary—to see that if these various systems of surveillance were under autonomous control outside of the capability of human intervention, the shift in practical authority would be magnified.

- To some, this speculative picture of the future is dystopian, and without appropriate democratic controls, it might be. But there are also utopian possibilities. The idea of mind control of an inanimate object, for example, lies at the core of possibly revolutionary prosthetic devices.

- A woman named Jan Scheuermann, who has been paralyzed from the neck down for years, had sensors embedded in the part of her brain that controls motion, and those sensors read electrical impulses and allow her to control a robotic arm. As a result, she can move objects and lift them. This is an example of how machine and humankind—metal and flesh—might extend our potential.

- IBM's stellar computer program Watson won a *Jeopardy!* game showdown against the greatest human champion to have ever played on the show, Ken Jennings. To prevail, the IBM program used deep learning and cognitive computing to understand natural language problems and to reason—to find the right answer.

- Today, IBM is taking that same deep-learning technology and deploying it to allow Watson to participate in health decisions. It can pull together vast quantities of data about health, disease, nutrition, lifestyle, and individual and collective medical histories.

- From that data, Watson can extrapolate and offer hypotheses about diagnosis and treatment in ways that are likely to lead to better health outcomes. All of which simply is another way of restating a basic premise of this course: that technologies are generally neutral. It is how they are employed that is of concern. And that means that our principal focus should be on questions of accountability and oversight.

Dichotomy in American Society

- The names Chelsea (formerly Bradley) Manning, Julian Assange, and Edward Snowden are now familiar to most Americans. Some think of them as heroes and patriots; others consider them villains and traitors.

- This dichotomy reflects the fundamental tension—the perpetual and unsteady equilibrium—between secrecy and transparency, between security and freedom, that pervades American society. In many senses, the tensions are ineradicable and inherent in the structure of American government. They require us to consider and reconcile two cherished values: limited government and effective government.

- Americans value limited government because humans value freedom and frequently think that government is as much a threat to freedom as it is an enabler of it. So, we value checks on government excess so highly that, for example, the right to freedom of speech is enshrined in the First Amendment.

- The converse of this—distrust of government—is a foundational insight of the Declaration of Independence, which is an assertion that the rights to life, liberty, and the pursuit of happiness are inalienable and belong to us by virtue of our humanity—and are not, in any way, derived from or granted by government. Likewise, we see rights of privacy and security against governmental intrusion as critical components of our rights as citizens.

- At the same time, we want a government that works, and works well. The desire for order and government protection from threats stretches at least as far back as the Hobbesian concern that without communal security, life is "nasty, mean, brutish, and short." That concern finds strong echoes in the constitutional preamble, which sets as one of the priorities that the new government "provide for the common defense."

- Before the Constitution, the new nation's first attempt to draft a blueprint for democratic government was something called the Articles of Confederation, which proved to be inadequate to the task. The Constitution itself was, therefore, a reaction against ineffective government and the chaos of an ungoverned society. Indeed, the framers of the Constitution sought to create a stronger government.

- Throughout U.S. history, Americans have confronted crisis with strong executive action—sometimes action that trenches close to, or crosses, the line of the law. Examples abound, ranging from President Abraham Lincoln's unilateral suspension of the writ of habeas corpus to President Franklin Roosevelt's covert aid to Britain in World War II in contravention of the Neutrality Act.

- More recently, and perhaps more controversially, we saw strong executive branch action in the wake of foreign terror attacks on U.S. soil on September 11, 2001. Our responses ranged from covert surveillance to military responses. But one thing unites many of these examples: the need, in some part, for secrecy in execution.

- Franklin Roosevelt's circumvention of the Neutrality Act to assist Britain during World War II would have been stopped had it been widely known to a still-isolationist Congress. Secrecy was also essential to the successful Navy SEAL operation targeting Osama bin Laden. In short, secrecy is sometimes crucial to effectiveness.

- But secrecy and transparency are often in equipoise: Too much transparency threatens security, and too much secrecy threatens liberty. Late in the Vietnam War, the unauthorized leak of the Pentagon Papers (involving the publication of a Defense Department analysis of the military campaign) reminded us that governments often use secrecy to conceal mistakes or misconduct—or simply to avoid embarrassment.

- The obligation of the government is a dual one: to protect civil safety and security against violence, and to preserve civil liberty. That dual obligation remains at the center of the surveillance/liberty debate.

- Americans want an effective government, but it has to be circumscribed by law and policy. This might present a false choice: that you can either have transparency, accountability, and liberty, or you can have secrecy, surveillance, and effectiveness. If we really were put to such a choice, it would be a difficult—indeed, almost existential—question to answer.

- But the United States can, and indeed does, reflect transparency and secrecy—accountability and effectiveness. Our goal should be to maximize both values.

Questions to Consider

1. How should autonomous learning machines be regulated and controlled? Who should bear the legal and practical responsibility for their operation?
2. Sometimes people say that the tension between secrecy and transparency is really a pendulum, swinging back and forth as one or the other idea takes hold. Do you agree? Where is the pendulum now?

Bibliography

Surveillance and Technology

Anderson, Kenneth, and Matthew Waxman. "Law and Ethics for Robot Soldiers." *Policy Review* (December 2012). http://www.hoover.org/research/law-and-ethics-robot-soldiers.

Baer, Martha, et. al. *Safe: The Race to Protect Ourselves in a Newly Dangerous World*. East-West Partners, 2005.

Bergman, Ronen. "The Dubai Job." *GQ* (January 2011). http://www.gq.com/story/the-dubai-job-mossad-assassination-hamas.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare*. Penguin Press, 2011.

Harris, Shane. *@War: The Rise of the Military-Internet Complex*. Houghton Mifflin Harcourt, 2014.

La Vigne, Nancy G., Samantha S. Lowry, Joshua Markman, and Allison Dwyer. *Evaluating the Use of Surveillance Cameras for Crime Control and Prevention*. Urban Institute, 2011.

Levine, Evan, and Jessica Tisch. "Analytics in Act at the New York City Police Department's Counter-Terrorism Bureau." *Military Operations Research* 19, no. 4 (2014).

Priest, Dana, and William Arkin. "Top Secret America." *The Washington Post* (September 2010). http://projects.washingtonpost.com/top-secret-america/.

Privacy and Civil Liberties Oversight Board. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. 2014. https://www.pclob.gov/library/702-Report.pdf.

———. *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*. 2014. https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

Rubinstein, Ira, Greg Nojeim, and Ronald Lee. *Systematic Government Access to Personal Data: A Comparative Analysis*. Center for Democracy and Technology, 2013.

Wittes, Benjamin, and Gabriella Blum. *The Future of Violence: Robots and Germs, Hackers and Drones: Confronting a New Age of Threat*. Basic Books, 2015.

History

Koehler, John O. *Stasi: The Untold Story of the East German Police*. Basic Books, 2008.

Larson, Erik. *In the Garden of Beasts: Love, Terror and an American Family in Hitler's Berlin*. Crown, 2012.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. 2004. http://govinfo.library.unt.edu/911/report/911Report.pdf.

Offices of Inspectors General. *Unclassified Report on the President's Surveillance Program (No. 2009-0013-AS)*. July 2009. https://fas.org/irp/eprint/psp.pdf.

Thomas, Evan. *The Very Best Men: Four Who Dared*. Simon & Shuster, 1996.

Weiner, Tim. *Enemies: A History of the FBI*. Random House, 2013.

———. *Legacy of Ashes: The History of the CIA*. Doubleday, 2007.

Political Theory and Practice

George, Roger Z., and Harvey Rishikof, eds. *The National Security Enterprise: Navigating the Labyrinth*. Georgetown University Press, 2011.

Goldsmith, Jack. *Power and Constraint: The Accountable Presidency after 9/11*. W. W. Norton & Co., 2012.

Heyman, Phillip. *Terrorism Freedom and Security: Winning without War*. MIT Press, 2003.

Ignatieff, Michael. *The Lesser Evil: Political Ethics in an Age of Terror*. Princeton University Press, 2004.

Rosenzweig, Paul. "Cybersecurity and Public Goods: The Public/Private 'Partnership.'" In *Emerging Threats in National Security and Law*. Edited by Peter Berkowitz. Hoover Institution Task Force on National Security and Law, 2011. http://www.hoover.org/sites/default/files/research/docs/emergingthreats_rosenzweig.pdf.

Rosenzweig, Paul, Timothy J. McNulty, and Ellen Shearer, eds. *Whistleblowers, Leaks and the Media: The First Amendment and National Security*. American Bar Association & Medill School of Journalism, 2014.

Privacy and Liberty

Bailey, Dennis. *The Open Society Paradox: Why the 21st Century Calls for More Openness—Not Less*. Brassey's, 2004.

De Villepin, Dominique. *Prevailing against Terrorism: White Paper on Domestic Security against Terrorism*. La Documentation Française, 2006. http://www.ambafrance-dk.org/IMG/pdf/livre_blanc_english.pdf.

Etzioni, Amatai. *How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism*. Routledge, 2004.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State*. Holt, Henry & Co. Inc., 2014.

Harris, Shane. *The Watchers: The Rise of America's Surveillance State*. Penguin Press, 2010.

O'Harrow, Robert, Jr. *No Place to Hide*. Free Press, 2005.

Reuter, Dean, and John Yoo, eds. *Confronting Terror: 9/11 and the Future of American National Security*. Encounter Books, 2011.

Rishikof, Harvey, Stewart Baker, and Bernard Horowitz, eds. *Patriots Debate: Contemporary Issues in National Security Law*. ABA Publishing, 2012.

Ronson, Jon. *So You've Been Publicly Shamed*. Riverhead Books, 2015.

Rosen, Jeffrey. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*. Random House, 2004.

Rosenzweig, Paul. "Whither Privacy?" *Surveillance & Society* 10, no. 3/4 (2012): 344–347. http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/whither/whither.

Solove, Daniel. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Press, 2011.

Wittes, Benjamin, and Jodie Liu. *The Privacy Paradox: The Privacy Benefits of Privacy Threats*. Brookings Institution, 2015.

Big Data and Cybersecurity

Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*. February 2012. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Post, David. *In Search of Jefferson's Moose: Notes on the State of Cyberspace*. Oxford University Press, 2009.

President's Council of Advisors on Science and Technology. *Big Data: Seizing Opportunities, Preserving Values*. Executive Office of the President, 2014.

Rosenzweig, Paul. *Cyberwarfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. Praeger Press, 2013.

Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Co., 2015.

Singer, Natasha. "You for Sale: Mapping, and Sharing, the Consumer Genome." *The New York Times* (June 16, 2012).

Law

Schmerber v. California, 384 U.S. 757 (1966).

Katz v. United States, 389 U.S. 347 (1967).

United States v. White, 401 U.S. 745 (1971).

United States v. United States District Court (Keith), 407 U.S. 297 (1972).

Branzburg v. Hayes, 408 U.S. 665 (1972).

United States v. Miller, 425 U.S. 435 (1976).

Smith v. Maryland, 442 U.S. 735 (1979).

United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

Department of Justice v. Reporter's Committee for Free Press, 489 U.S. 749 (1989).

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

Gilmore v. Gonzales, 435 F.3d 1125 (9th Cir. 2006).

Quon v. City of Ontario, California, 560 U.S. 746 (2010).

In Re Grand Jury Subpoena (United States v. Doe), 670 F.3d 1335 (11th Cir. 2012).

United States v. Jones, 565 U.S. ___, 132 S.Ct. 945 (2012).

Maryland v. King, 569 U.S. 2013, 133 S.Ct. 1958 (2013).

Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014).

Riley v. California, 573 U.S. ___, 134 S.Ct. 2473 (2014).

Google v. Spanish Data Protection Authority and Mario Costja Gonzalez, European Court of Justice (Grand Chamber) (May 2014).

Contemporary Blogs

American Bar Association Standing Committee on Law and National Security. www.americanbar.org/groups/public_services/law_national_security.html.

Just Security. www.justsecurity.org.

Lawfare. www.lawfareblog.com.

Image Credits

Page 7: © Rena Schild/Shutterstock.
Page 12: © AdrianHancu/iStock Editorial/Thinkstock.
Page 15: © Digital Vision/Photodisc/Thinkstock.
Page 19: © Sean Gallup/Getty Images News/Thinkstock.
Page 25: © Richard Cavalleri/Shutterstock.
Page 31: © Rob Wilson/Shutterstock.
Page 35: © Public Domain/Wikimedia Commons.
Page 43: © ID1974/Shutterstock.
Page 47: © everything possible/Shutterstock.
Page 51: © Anthony Correia/Shutterstock.
Page 55: © David Molina G/Shutterstock.
Page 63: © frank_peters/Shutterstock.
Page 68: © frank_peters/Shutterstock.
Page 77: © Tyler Olson/Shutterstock.
Page 85: © Rawpixel/Shutterstock.
Page 91: © Kekyalyaynen/Shutterstock.
Page 95: © Leonard Zhukovsky/Shutterstock.
Page 98: © Denys Prykhodov/Shutterstock.
Page 105: © Jacob Lund/Shutterstock.
Page 111: © Cyril Hou/Shutterstock.
Page 122: © Zerbor/Shutterstock.
Page 125: © GongTo/Shutterstock.
Page 131: © weedezign/Shutterstock.
Page 139: © LoloStock/Shutterstock.
Page 144: © Rena Schild/Shutterstock.