AFTER SNOWDEN

PRIVACY, SECRECY, AND SECURITY IN THE INFORMATION AGE

RONALD GOLDFARB, EDITOR

THOMAS DUNNE BOOKS

ST. MARTIN'S PRESS

NEW YORK

Thank you for buying this
St. Martin's Press ebook.

To receive special offers, bonus content,
and info on new releases and other great reads,
sign up for our newsletters.

Sign Up

Or visit us online at
us.macmillan.com/newslettersignup

For email updates on the editor, click here.

INTRODUCTION

RONALD GOLDFARB

RONALD GOLDFARB is a veteran Washington, D.C., attorney, author of thirteen books, and a literary agent. He worked in the Department of Justice prosecuting organized crime cases during the Kennedy administration, and served as trial counsel in the U.S. Air Force, JAG, for three years before that. He was special counsel to a congressional (House of Representatives) investigation, and was appointed to chair a special review committee established by a D.C. federal court dealing with the practices of the Department of Labor. His Web site, http://www.ronaldgoldfarb.com, lists his biography in full detail.

THE NOTORIOUS REVELATIONS of Edward Snowden, former U.S. government employee and contractor, who stole and made public a deluge of classified government documents concerning U.S. surveillance practices, have generated passionate reactions worldwide. Most people have strong opinions about whether Snowden is a megalomaniacal traitor or a self-sacrificing patriot, and whether our nation's policies should err on the side of protecting national security or civil liberties. Use of the word "leak" to describe Snowden's disclosures, rather than geyser or waterfall, is as minimalizing of his action as the charge of espionage by the government seems a grandiose exaggeration of his offense.

Mediating the debate over the right judgment of Mr. Snowden's behavior is not the aim of this collection of essays by eminent scholars with expertise in relevant fields affected by the Snowden affair. Whatever the final verdict on Snowden may be—whether he is a public-spirited whistleblower, classic leaker, actor in a proud tradition of civil disobedience, or a vain and reckless vigilante, a treacherous criminal who has hurt his country—his behavior has raised important questions about our nation's dragnet surveillance practices and the proper agencies and manner of its review. These questions are the subject of this book.

What are the proper bounds of secrecy? Are current government surveillance practices justified as necessary measures of national security at a time of extraordinary provocation, or do they go too far, setting a dangerous precedent for our national policies of self-protection that could lead to a security state? And if so, who decides that, and what should be done about it?

A high school dropout and technical wizard, Snowden worked for the CIA, NSA, Defense Intelligence Agency, and recently for a private contractor (first Dell, then Booz Allen Hamilton) commissioned by the NSA, doing what has been described as cyber-counterintelligence. Once an idealistic participant in U.S. national security programs, Snowden became disillusioned by what he perceived as government excesses and abuses in its data gathering. Believing that he had no proper alternatives, Snowden fled from his carefree life in Hawaii, his well-paying job, his girlfriend, and his country, taking along four laptops with encrypted, top secret files. He claims he did so in order to protest what he viewed as major incursions on people's privacy and constitutional rights. "I took an oath to support and defend the Constitution and saw that the Constitution was being violated on a massive scale," he told a Texas teleconference.[1]

The Snowden Files, by *The Guardian* editor Luke Harding[2]—to be a movie by Oliver Stone—described the exciting, intense behind-the-scenes story of Snowden's dramatic flight to Hong Kong and his secret meetings with lawyer-journalist Glenn Greenwald, author of *No Place to Hide.*[3] Greenwald's book complements and expands on Harding's story, as does the work of documentary filmmaker Laura Poitras—Snowden's other chosen vehicle for telling his story to the world. Poitras's Academy Award–winning documentary covering that clandestine drama, *Citizenfour* (Snowden's code name for Poitras), was shown in New York City on October 2014.[4] *New Yorker* columnist George Packer called it "a political thriller." Poitras considers it a "human drama."[6] The prize-winning reporter Barton Gellman would later join them in telling Snowden's story at *The Washington Post.*

For ten intense, perilous, around-the-clock days in Hong Kong, the three met secretly in Snowden's room at the Mira Hotel, joined by *The Guardian*'s expert on national security, Ewen MacAskill, to evaluate Snowden's story before they would eventually tell it to the world. Once satisfied with Snowden as a credible source (after forty-eight hours of "speed dating," as MacAskill called it),[5] *The Guardian* called the White House seeking a quick response before going public with Snowden's material. Getting none, *The Guardian* broke the story. Snowden hurriedly departed Hong Kong for refuge in South America, but finding his passport canceled by the United States ended up grounded en route at the airport in Russia.

At this time, Snowden, a thirty-one-year-old man without a country, remains in Russia under temporary asylum, recently joined by his girlfriend, regularly interviewed by visiting reporters, and broadcasting his story and viewpoints to audiences worldwide over the Internet. His residence permit recently was extended for three more years, as he negotiates safe harbor in other countries, evading extradition and facing an indictment in the United States for espionage and theft of government property for which he faces thirty years in prison. Reviled for recklessness and praised for self-sacrifice, his actions already have generated the beginnings of reforms.

Through his trusted journalistic confederates, he continues to expose the government's questionable surveillance practices. He certainly has generated a national debate about this subject in the United States, and engaged other countries in an international conversation by raising the public's consciousness about the practices of surveillance in the borderless world of cyberspace. In October 2014, the UN's top counterterrorism and human rights official formally reported to the General Assembly that questionable electronic surveillance by member states unjustifiably violated core privacy rights in violation of multiple treaties and conventions. Reformative bills are pending before the U.S. Congress. Reevaluation of House and Senate oversight practices are underway. Lawsuits have been filed. A high-level White House review

panel already has proposed forty-six reform measures.

The Snowden affair raises a classic, fundamental question about how our three branches of government should synchronize their work, yet check and balance each other's powers. Is the executive branch's work on national security—arguably no more important role exists as part of its constitutional powers—properly overseen by the Congress and the courts? And how does the press monitor all three branches when national security is the question? Have surveillance technologies "outpaced democratic controls," as one of Snowden's attorneys claimed? A recent *Foreign Affairs* article concluded that "Snowden's revelations demonstrated how the implicit bargain that has governed the U.S. intelligence community since the 1970's has broken down." Has it? How so? What to do about it?[7]

This book aspires to inform the debates generated by the Snowden disclosures about critical policies: the role of the press in reporting about national security; the value of leaks and the need for whistleblowers; the proper bounds and treatment of civil disobedience; the roles of courts and Congress in overseeing executive practices taken in the defense of our nation; and the appropriate balance between privacy and government investigation and secrecy in this evolving era of invasive technology and metadata gathering.

How do we protect our nation's security without creating, in the words of Cato Institute official Julian Sanchez, "a nigh-omniscient, planet-spanning, electronic panopticon"?[8] And how do we deal with the conundrum described by James Clapper, Director of National Intelligence?: "We are supposed to keep the country safe, predict anticipatory intelligence, with no risk and no embarrassment if revealed, and without a scintilla of jeopardy to privacy of any domestic person or foreign person. We call that 'immaculate collection.'"[9]

* * *

In the history of the United States—it could be said so about most, if not all, places—when national security, domestic terror, and personal provocation clash with people's civil liberties, the former prevail. That is human nature. The Constitution is not a suicide pact, the late Supreme Court Justice Robert Jackson said, capturing the human dilemma of this conundrum.[10,11] As Professor Jon L. Mills points out in his chapter, "The Future of Privacy in the Surveillance Age," the first words of the Constitution pronounce the need for national security. Over a century later judges declared that privacy, not a word that appears in the Constitution, is constitutionally protected by implication from other protections in the Constitution.

There is both wisdom and cynicism in the manner in which national security is enforced. A book, *America's War Machine*, by the late James McCartney and his wife,

Molly, both experienced reporters, quoted a remarkable conversation that took place in 1946 after World War II that echoes today in the wake of 9/11 and this country's attempts to prevent its recurrence.

> *"… it is always a simple matter to drag the people along, whether it is a democracy or a fascist dictatorship…," the speaker said.*
>
> *But in a democracy, his questioner argued, "… the people have some say … through their elected representatives, and in the U.S. only Congress can declare wars."*
>
> *The challenged interviewer responded: "Oh, that is all well and good, but voice or no voice, the people can always be brought to the bidding of the leaders. That is easy. All you have to do is tell them they are being attacked and denounce the pacifists for lack of patriotism and exposing the country to danger. It works the same way in any country."*

Ironically, the commentator quoted by the McCartneys was Hermann Goering, then a Nuremberg prisoner in an interview just before his execution. Some moral tutor to instruct on realpolitik![12]

History provides comparisons to current dilemmas—the internment of Japanese American citizens after the treacherous attack on Pearl Harbor, Hawaii, on December 7, 1941, was not one of this country's finest hours, and the infamous attack on America on 9/11 gave rise to draconian measures of extreme rendition, rationalized by some as necessary for national security, but condemned by others as excessive torture. In both instances, the provocation was clear, but the methods of response were questionable.

Materials provided by Snowden to Glenn Greenwald (reported in *The Daily Beast* and *The Intercept*) reported that the NSA and the FBI were monitoring e-mails of prominent Muslim Americans under secret procedures for targeting terrorists and foreign spies.[13] Should ethnic profiling of American Muslim citizens today be condoned as a rational necessity, or compared with the excessive intelligence gathering of civil rights and antiwar activists of the 1960s and 1970s, and alleged Communist movie figures in Hollywood in the McCarthy era?

There will be inevitable victims of investigative abuses in trying times, to be sure. No one questioned the deceptions and spying we and our allies performed during World War II in the war against fascism; indeed we romanticize what the OSS accomplished at Bletchley and elsewhere to bring down our fascist enemies by any means or tactics. The government's specific rationale for the particular practices Snowden has questioned is classified, and therefore impossible to assess. Presumably the rationale is that after 9/11 extreme precautions were prudent, necessary.

The policing of government at its highest precincts is a tricky but vital assignment. The late New York University law professor Edmond Cahn argued, in *The Predicament of Democratic Man* (1961), that misconduct by the government is more pernicious than that of individuals. We are all morally involved in the wrongs of government. Undermining the rule of law, which is the bedrock of democracy, is the ultimate crime, Professor Cahn posited, because it leads to anarchy and the police state.

That notion is the premise of Snowden defenders, that whatever his offense may have been, the official misconduct he revealed is worse. When James Clapper, our Director of National Intelligence, was asked at a Senate inquiry—pre-Snowden disclosures—if NSA collected data on Americans, he said under oath, "No, not wittingly," a perjury in the view of some critics, though no one has called for his indictment. Nor has there been criminal action taken against CIA employees who reportedly improperly surveilled U.S. Senate personnel and records. Senator Ron Wyden reportedly knew Clapper's remarks were false, but prevailing confidentiality rules forbade his challenging them publicly. "If the American people knew what I knew," he was quoted as saying, "they would be angry and they would be shocked."[14]

The efficacy of congressional oversight of the executive actions of seventeen separate agencies in national security matters became a matter of heightened public interest in the wake of Snowden's actions. How effective can congressional oversight be? For there to be synchronicity between branches of government, there needs to be trust between the congressional committees performing oversight and the executive agencies they oversee. Legislators have full plates of responsibilities. They rely on special committees and on their staffs and experts, some with more expertise and longevity and time than the members they serve. But they can probe only so far without the risk of spoiling the relations they depend on. Trust, but verify, works only insofar as one can verify.[15]

Dealings are not always collegial between the overseers and the overseen. The CIA inspector general reported that, in July 2014, CIA Director John Brennan apologized to Senator Dianne Feinstein for "spying on the senator's activities," in regards to her investigation of the CIA's torture practices in this instance.[16] No surprise, Senator Feinstein, a chief senatorial watchdog of executive surveillance practices, expressed pique at the interference with her committee staff by agents of those executive officials her committee was authorized to oversee.

Historically, some managers of congressional oversight didn't want to know what was going on and gave security agencies carte blanche. When he was Armed Services Committee Chairman, the late Senator John Stennis told CIA Director James Schlesinger in 1973 concerning the CIA's activities abroad, "No, no, my boy, don't tell

me, just go ahead and do it but I don't want to know," according to Loch Johnson's history of intelligence oversight.[17],[18]

In the 1970s, this attitude changed, but after 9/11 the national security apparatus ramped up, understandably. In the follow-up of the Snowden affair, congressional experts and critics are reexamining the effectiveness of Congress acting as proxies for the American public in overseeing the intelligence community, and legislation is pending to rein in NSA's surveillance practices.

If there was greater professionalism by Congress in exercising its oversight responsibility—for example, a joint select committee and super staff for national security matters—as the 9/11 Commission recommended, would that improve the status quo? The 9/11 Commission stated:

> *Of all our recommendations, strengthening congressional oversight may be among the most difficult and important. So long as oversight is governed by current congressional rules and resolutions, we believe the American people will not get the security they want and need. The United States needs a strong, stable, and capable congressional committee structure to give America's national intelligence agencies oversight, support, and leadership.*[19]

A 2006 report by the Center for American Progress, *No Mere Oversight*, prepared by national security veterans, concluded that congressional oversight has been dysfunctional: "Congress has all of the tools it needs; it is simply not using them." The process has become "paralyzingly partisan," needs to be prodded by the press to deal with abuses, and is hampered by lack of cooperation "all but non-existent today" between congressional committees with different responsibilities. Congress largely defers to the executive, the report states. Congress is in an awkward position because there is a difference between what its members can say in public and in classified briefings.[20]

How does Congress know about what intelligence agencies are doing? The CIA and NSA require a written finding from the uppermost echelons of the executive branch before it carries out its surveillance programs. Congress knows that, and the budget breakdowns report the funding of these programs, even if code words are used in describing sensitive areas. Therefore, it appears unlikely that at least the top congressional intelligence members did not know about the surveillance programs Snowden revealed. Or that the private companies the PRISM data-mining program exploited did not go to those congressional officials to complain. We, the public, can't know the answer, of course.

A former congressional official told me that, even if it is counterintuitive, considering the scale of the surveillance procedures now in question, it is possible no

one in our Congress was aware of them.[21]

However, a knowledgeable, retired CIA and Senate intelligence official advised me that the law requires committees to be "fully and currently informed," and that the intelligence agencies are required to inform the committees about covert action. They fail to do so "at their own peril," he concludes. In his experience, both on the committee and in the intelligence agencies, "… the agencies generally make a good-faith effort to tell the committees what they are doing, *especially* if it appears to be problematic to them. They don't want something to blow up in their faces and have the committees pissed off that they were never notified. They want buy-in from the committees because it protects them."

Nevertheless, the 9/11 Commission concluded that legal oversight for intelligence and counterintelligence is now dysfunctional. It interviewed members of Congress and staff and reported that "dissatisfaction with congressional oversight remains widespread." Few members have the necessary knowledge of intelligence work, the Commission concluded.

This criticism does not mean that Congress has failed to act to improve its oversight practices in recent years, one experienced insider advised me. It has required an array of additional oversight measures: notification of executive intelligence activities, added financial oversight and improved appropriations and authorization processes, and created the position of inspector general in intelligence agencies. These inspectors are authorized to work with whistleblowers, respond to press pressures, and oversee the minimization of excessive practices.

Another former intelligence official suggested that as a practical matter, the controversial programs Snowden disclosed may be curtailed for economic reasons, especially if their utility is of dubious value. Further, he speculates, there may be worse incursions of privacy by local and state police officials whose gathering and collating of their terrorism surveillance are likely to be available to federal intelligence agencies.

Still another expert suggested that one of the problems with the post-9/11 national security process is that the NSA hired many contractors to do what its employees did in the past. That led to hires, like Snowden, who had access to highly sensitive materials. The agencies were not as careful about hiring outside employees as they had been in the past, this former high CIA and Senate official told me. And further, he added, political polarizing has hurt the oversight function, adding mistrust and uncertainty to the process of synchronization of congressional and executive branch officials in this sensitive field.

New Yorker political analyst Ryan Lizza spelled out the background politics of congressional oversight in detail in "State of Deception" (December 16, 2013). While

the Intelligence Committee was created in the 1970s to provide "vigilant oversight of the intelligence community," he noted, there have been and still are differences in congressional members' views of their responsibility. Currently there are those who believe the Committee is too beholden to the officials they oversee. Congressman Jim Sensenbrenner, one author of the Patriot Act, wrote in August 2013, "I did not know the administration was using the Patriot Act (Section 215) for bulk collection and neither did a majority of my colleagues." Others, the majority, are deemed by critics to be solicitous, sometimes deferential to the expertise of executive officials in the intelligence community.

Lizza's behind-the-scenes depiction of how, up to the present, the Department of Justice, the White House, and even the Foreign Intelligence Surveillance Act (FISA) courts have gone along with intelligence excesses, even when some had criticisms of them, is daunting. He concludes his analysis: "… given the history of abuse … it's right to ask questions about surveillance—particularly as technology is reshaping every aspect of our lives."

James Risen's *Pay Any Price* describes a revealing incident that demonstrates the weakness of congressional oversight. A NSA official advised Diane Roark, a staff member of the House Permanent Select Committee on Intelligence, that a domestic surveillance program was potentially unconstitutional and he couldn't persuade his colleagues of its danger. Roark agreed and questioned NSA Director Michael Hayden about this, and he resisted her entreaties, stating that high congressional officials and lawyers "from three branches" had been informed of and approved the program. She raised the question with her Committee colleagues and was told to drop the matter. She called a FISA judge, who didn't talk to her but reported her call to the Department of Justice. Everyone she called seemed to accept the executive decision that the program was legal. Roark was told by Hayden that if challenged they "have the majority of nine votes," the Supreme Court, presumably. Risen wrote: "She had gone to all three branches of government … and had discovered that there was a conspiracy of silence … to protect an unconstitutional operation." Roark resigned her job and moved to Oregon.[22]

Bottom line, it is unfair to criticize national security agencies alone for these now controversial programs. The public elects representatives in Congress to oversee the executive. Periodically, the question whether the constitutional tripartite function of our government is working as it should be is up for consideration. One history of intelligence oversight concluded that it has gone through five phases—eras of trust, uneasy partnerships, distrust, partisan advocacy, and congressional acquiescence. Historically, and to this day, the pendulum swings favoring different demands, different emphases, as events change. Where will it—should it—go after Snowden?

There is a fundamental quandary separating those who favor erring in favor of national security and those concerned about invasions of personal privacy in times of conflict. Everyone sensibly favors national security *and* personal privacy. National security specialists argue there is no proof that their practices damaged anyone; and civil libertarians argue that the mere fact of the incursions alone *is* the damage.

Florida Senator Bob Graham, now retired, chaired the Senate Intelligence Committee for a decade at the end of the last century and the beginning of the present one. He wrote about congressional oversight in *Intelligence Matters* in 2004. Graham chaired the post-9/11 joint congressional committee inquiry into intelligence activities. Until the mid-1970s, he wrote, "Congress interfered as little as possible and trusted our intelligence agencies as much as possible." The CIA and the FBI failed to communicate with each other, and the executive branch had a blank check after 9/11, Graham wrote, as the intelligence process was politicized. Information was overclassified, he complained, and as a result "the public had its vision shrouded."

Graham pointed out that the Bush administration practiced "incestuous amplification," where people sharing the same point of view were making decisions. Graham believes that congressional oversight requires more expertise in Congress and avoiding too close an association with agencies it oversees. The December 2002 Joint Inquiry recommended, among other specifics, "the need to enhance national security while fully protecting civil liberties." It also pointed out that classification can impair congressional oversight, as it may shield self-interest.

The lessons Graham advocates are relevant today. Complaining about excessive secrecy, Graham pointed out, "The public can't respond to things it isn't told, or seek reforms to problems it is kept from seeing." Prophetically, he added, "America must decide how much domestic security they will accept and the inevitable intrusion that it will cause on our individual civil liberties. The debate on that balance has yet to begin."

I asked Senator Graham how congressional oversight might be improved in the wake of the Snowden affair. He doesn't think, as the 9/11 Commission suggested, that structural change is needed. He believes improvement will come with more qualified and aggressive members and a unified nonpolitical professional staff. As much as politics can be taken out of the mix, the better; though that is unlikely in such an essentially political institution. Graham is critical of the insularity and competitiveness of the executive agencies managing surveillance, which can result in missed opportunities to prevent terrorism, as has happened. In the final judgment, however, Graham agrees that there is a fundamental problem in oversight when, as is the case, the overseer must rely on the overseen: "You don't know what you don't know."

Congress does not seek to and ought not manage national security, so oversight is

reduced to watchdogging and reforms after the fact. Congress can do something about Snowden's revelations now if it wants to, but can it ever prevent excesses from happening before they happen? Or must Congress ultimately defer to executive branch practices, relying on its expertise and on the courts to perform judicial oversight? Professor Barry Siegel's "Judging State Secrets" suggests that relying on judicial oversight is illusory, or has been in modern times. Judiciary Committee Chairman Senator Patrick Leahy has noted, "The press is doing our work for us and we should be ashamed of it."

* * *

Critics of Snowden argue that if every rogue government employee was free to decide when and whether to violate his duties and commitments, we would have nihilistic anarchy. If our government cannot insure domestic tranquility and provide for the common defense, as the Constitution declares in its opening passage, there will be no democracy, no surviving society, no "perfect union," and ultimately, no Constitution. Snowden admits he signed an agreement, Standard Form 312, subjecting him to civil sanctions and the risk of jail, when he took his job.

How did our country's defenders become the accused offenders in performing their important work, and Snowden suddenly a hero, to some, for what others claim was treacherous malfeasance? For one reason, as Professor Mills points out, the national security apparatus decided, in the frightening aftermath of 9/11, to go after our enemies, even if it meant "collecting the haystack" in search of the dangerous needles within it. At times of threats like this, the public understandably defers to its government to do whatever is necessary to defend us, no-holds-barred.

But secrets rarely remain secrets, and inevitably there is exposure and pushback. In his recent novel, *The Director,* David Ignatius's antihero, reminiscent of Edward Snowden, is a fugitive in Caracas who has leaked secret U.S. government records. His credo is not unlike some real-life, new-generation geek hackers and rogue patriots—or pseudo-patriots, in some eyes—who decide for themselves what is good and evil, moral and immoral, and take pride in doing it:

> *"I didn't kill anyone. I didn't torture anyone. I didn't listen to people's telephone calls or steal their secrets. They claim that I broke the laws of the United States, but I didn't break any of the laws of humanity. I left the CIA as an act of conscience. I revealed its secrets to give liberty to others."*[23]

The question, as we see it, is not whether the executive branch of our government should take all proper steps to guard the security of the nation—of course it should. But what are the proper bounds of those steps? And who gets to say so? And how

should that be accomplished and monitored in the public's interest?

* * *

The NSA was created by President Harry Truman in 1952 to coordinate government surveillance after WWII. It is a military agency that reports to the Director of National Intelligence. In response to congressional disclosures of intelligence gathering excesses (the Church Committee) in 1978, Congress enacted FISA to oversee domestic surveillance practices by a special secret court. The effectiveness and fairness of this method of judicial review of executive activities (rarely denying government requests for warrants, or hearing an opposing argument) has been questioned, as bordering on ministerial rather than judicial. The failure of judicial review in national security cases is demonstrated in Professor Siegel's chapter.

Professor Mills's chapter details how after 9/11, the Patriot Act widened the scope of prior authorized government surveillance practices. Under Section 505, National Security Letters (NSLs) were issued by the FBI to communications providers, banks, phone companies, and Internet companies, demanding their data and forbidding them from revealing that fact. In effect, they are administrative subpoenas, needing no prior judicial approval, though they later can be and have been challenged in courts. Section 215 of the Patriot Act was the basis of a FISA ruling that Verizon data could be collected, procedures which the President's Oversight Board called an "impermissible" interpretation.

Litigation questioning the constitutionality of these NSLs disclosed the FBI had issued 56,000 of them, *Frontline* reported. The gag order provision of the NSLs under the Patriot Act has been challenged in federal courts as a violation of the Fourth Amendment. A bill reforming this practice as it pertains to U.S. citizens was proposed by President Obama and passed by the House. It is pending in the Senate.

A distinction has been made between the collection of metadata and content, suggesting that the former is less invasive of personal privacy than the latter, and doesn't necessarily require warrants. But critics, even the former general counsel to the NSA, point out, "If you have enough meta data, you don't really need content." One commentator cited a hypothetical example. If a husband calls his wife to say he is working late, his remarks to her are the content. But the metadata might show that the call came from a motel, following an earlier call to an escort agency (ZDNet, September 16, 2014).[24]

The Bush administration acted on the theory that presidential power under Article II, Section 2, of the Constitution itself allowed additional means of collecting information in time of "war." Executive Order 12333, issued in 1981 by President Reagan, expanded the essentially secret collection of intelligence overseas on

foreigners. The reach of this surveillance practice is vast, and includes data not reviewed by courts or Congress because it targets foreigners, though it dragnets American citizens in the process under FISA, Section 702, which became the basis for the collection of data of U.S. citizens, too. The evolution of all these laws is analyzed by Professor Jon Mills in his chapter.

An additional wrinkle was reported by former State Department official John Napier Tye in a *Washington Post* article in July 2014.[25] His article, "reviewed and cleared" by the State Department and the NSA, states that Section 215 of the Patriot Act authorizing the government to obtain court orders to compel private telecommunications companies to turn over phone data is not the whole story. It does not include the collecting and storing of U.S. communications, which is covered by Executive Order 12333. That order, not a law and not subject to judicial review or congressional oversight, allows collection of content, not only the gathering of metadata, of U.S. citizens, even if it is "incidentally" collected overseas. That "loophole," Tye pointed out, "can be stretched very wide."

Since U.S. communications travel across U.S. borders routinely, the NSA can collect and store the content of communications between U.S. citizens gathered outside the United States as part of a foreign intelligence investigation, without a warrant or court order and without Congress knowing about it. Senator Dianne Feinstein, chairman of the Senate Select Committee on Intelligence, stated that her committee cannot oversee conduct covered by Executive Order 12333. Nor does the NSA need to advise the private companies collecting this data that it is doing so.

Tye reports that he advised the State Department inspector general, NSA's inspector general, and House and Senate intelligence committees that he thought 12333 violates the Fourth Amendment's unreasonable search and seizure prohibition. He discussed his view with a member of the President's review group appointed after the Snowden disclosures and was advised that it had recommended (Rec. 12) that all data of U.S. citizens incidentally collected be "purged unless it has foreign intelligence value or is necessary to prevent serious harm." Tye was told by White House staffers there were "no plans to make such changes."

Tye argues that it makes no sense that U.S. citizens should have weak privacy protection when their communications are collected by their government outside the United States. In words reminiscent of Snowden's (who, unlike Tye, did not try first to go through all available official channels with his complaints), Tye protested:

> *I am coming forward because I think Americans deserve an honest answer to the simple question: What kind of data is NSA collecting on millions, or hundreds of millions, of Americans?*

The USA Freedom Act, passed by the House and pending in the Senate, would reform FISA practices and end bulk collection of phone records, as the President and intelligence chief James Clapper proposed after Snowden's disclosures of PRISM became public. Microsoft's general counsel Bradford Smith recently told a Harvard Law School audience that the FISA court should be reformed. However, that act hasn't been passed, and proponents fear that, given the current reemergence of worldwide terrorist activities, the public pressure for limiting intelligence gathering will fade.

* * *

How did all this happen? There was understandably "a profound shift in national security priorities" after 9/11, which combined with a "tectonic shift" caused by advances in technology. We now know that in addition to its own surveillance, the NSA appropriated data from nine private Internet companies, capturing "enormous flows of data at the speed of light from fiber optic cables that carried Internet and telephone traffic over continents and under seas," Pulitzer Prize–winning journalist Barton Gellman reported, based on his interviews with Snowden.

Those private Internet companies, like Microsoft, acknowledge their duty to comply with legal orders and judicial dictates, but were outraged by being seen as "candy stores for U.S. intelligence," Gellman noted. Where there is probable cause to target people for proper intelligence purposes, doing so is legitimate. Yet *The Wall Street Journal* reported that roughly 75 percent of all U.S. Internet traffic is vacuumed by the U.S. surveillance programs, including private communications of both U.S. and foreign citizens. Intelligence Committee member Senator Ron Wyden told Silicon Valley executives that the government's "digital dragnet" created a clear and present danger for the Internet economy without making the country safer.[26]

Microsoft's general counsel Bradford Smith and his otherwise competitive legal counterparts at Google, Facebook, Twitter, Apple, and LinkedIn recently formed a coalition, Reform Government Surveillance, to push for government changes to its appropriation of online social media data. Those companies, along with Yahoo, Microsoft, and Dropbox, signed an open *New York Times* letter calling for stronger congressional controls. Private companies are concerned about their image, and the economic impact of these surveillance practices on their business, as well as the constitutional implications. Their awareness has heightened as a result of the Snowden disclosures. For example, Yahoo has improved its security practices and other companies are taking more care of data security through encryption. New companies in Switzerland and Germany are developing NSA-proof encryption products to exploit this new market.

Government officials have expressed fears that encryption devices developed by

Apple and Google in the wake of Snowden's disclosures will adversely affect law enforcement. As a result of Snowden's exposure of the PRISM program, Google and Apple (96.4 percent of the smartphones in the world) have developed encryption techniques to avoid intrusions. The new head of Government Communications Headquarters (GCHQ) in Britain, along with the FBI and the New York City district attorney, complain that this will preempt search warrants and thus impair necessary law enforcement. Snowden says that, after a warrant is issued, encrypted material and geo-location data can be accessed from the cloud. And he told Harvard law professor Lawrence Lessig that backdoors in any system can be accessed by savvy intruders, not only law enforcement officials. Snowden advocates an international Magna Carta for the Internet governing digital rights worldwide.

The Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires traditional phone companies to include lawful intercept capabilities. The FBI is seeking its expansion to other companies as a law enforcement necessity. Civil liberties organizations and software manufacturers argue that weakening encryption makes citizens vulnerable to hacking by criminals and foreign governments. That seesaw debate will continue until a balanced compromise is found.

Economic considerations merge here with ethical ones. Bloomberg News reported that technology companies fear losing $35 billion in the next three years from foreign customers who choose not to buy U.S. products because these companies cooperated with spy programs (July 2014). However, a *Forbes* magazine report suggested these private companies "don't look to be suffering from any kind of mass exodus" (April 15, 2014). *Politico* added, "Nations and companies have too much invested in the global Internet to let it balkanize," as different countries are motivated to apply rigorous safeguards to prevent excessive surveillance protection (June 5, 2014).

The release in September 2014 of 1,500 pages of formerly classified sealed documents made headlines because they showed that the government had ordered Yahoo to make its customer records accessible, and threatened to fine the company $250,000 *a day* if it refused to comply. It would have bankrupted the company to dispute the government's demands. The government acted under the earlier Protect America Act of 2007 and later FISA 2008 Amendments. Yahoo argued unsuccessfully before trial and appellate FISA courts that doing so violated its customers' Fourth Amendment rights. As a result of this defeat, other tech companies capitulated to the PRISM program providing for warrantless orders.

While Google, Yahoo, Microsoft, LinkedIn, and Facebook have settled with the government, Twitter is suing in the Ninth Circuit (Northern District, California), challenging the nondisclosure provision of the NSLs on First Amendment grounds. Twitter argues that it has been subjected to prior restraint, in effect a gag order, which

requires preapproval of its company reports, or refraining from any comments at all to its customers about government surveillance of its reports. The government contends that this information is classified.

The irony is, as a recent *Frontline* documentary on PBS described,[27] the private sector companies who surveilled their subscribers for advertising and economic purposes learned that the government was accessing their stored data for national security purposes through advanced tracking techniques.

Snowden advocates that there should be no constitutional "distinction between digital information and printed information." Yahoo's new security consultant reports that "[p]rivacy is much more effective as a selling point than it used to be." Professor Mills's chapter traces the law of privacy from the ideas of the progressive Justice Louis Brandeis of an earlier era to that of the current conservative Chief Justice John Roberts, demonstrating that the Constitution, then and now, protects personal privacy.

* * *

Resort to the Espionage Act for disclosures in the press, as is threatened in the Snowden matter, is rare. During World War II, *The Chicago Tribune* was investigated, but not indicted, for reporting secret government naval intelligence. It ran antiwar stories mentioning our breaking encrypted Japanese messages about its armada at Midway in 1942, and an account on December 6, 1941, of U.S. military plans in Europe. The government threatened, but backed off, indicting *The Tribune* under the Espionage Act of 1917. One can hardly imagine a situation more warranting of prosecution than the disclosure of secret wartime maneuvers. The only example of a successful prosecution for press behavior involved Samuel Morison's publication in *Jane's Defence Weekly* of three classified photos of a Soviet nuclear submarine. He was convicted under the Espionage Act, served two years in prison, and was pardoned by President Clinton. In other cases involving the Espionage Act, such as the notorious Rosenberg and Pollard cases, disclosures had been made to foreign countries (one hostile, the other friendly), but that was not the case here.

The press usually prevails in comparable clashes with the government, more so than lone individuals. When the notorious Pentagon Papers were leaked and published by *The New York Times* and *The Washington Post,* despite government arguments that this endangered America's interests, the U.S. Supreme Court refused to enjoin publication of that Vietnam War history. It was a cause célèbre and became a landmark victory for freedom of the press.

The role of the press is critical when intragovernment checks and balances don't work. The digital press changes and speeds up this process. In the Snowden case there was an ironic element. Snowden distrusted the establishment press and sought out

Greenwald, Poitras, and Gellman for that reason, but they all realized that without the resources of the establishment press their story would lack the impact they sought. First, they reached out to *The Guardian.* While it broke the story, *The Guardian* was pressured by United Kingdom government officials who actually came to their offices and destroyed *Guardian* computers. *The Guardian* then made a deal with *The New York Times* (we have the thumb drives, they said to their new press partners, but you have the First Amendment, which protects us better than British law). Barton Gellman and *The Washington Post* also were brought in, and Gellman's stories have been prominent.

Even then, Glenn Greenwald complained in his book that the establishment media was timid, risk averse, not as adversarial with the government as he thought it should be, and that some of its members treated him and his extraordinary stories with cynicism while others seemed protective of the government. Hodding Carter, a former newspaper editor and later government spokesman for the State Department, discusses the role and responsibilities of the press in tense situations like Snowden's in his chapter, "The Press."

Snowden's revelations have caused a furor abroad, as well as in the United States. Brazilian President Dilma Rousseff protested after learning that her personal conversations were monitored, along with other officials in the world, whether they be foreign allies or enemies (i.e., Iran, Turkey, Venezuela, Cuba, China, Russia). Australia and Indonesia formed a new agreement on their spying practices. Former Israeli Prime Minister Ehud Olmert learned his phones and e-mails were tapped, though Israel and the United States, however close their relations, are known to spy on and share information with each other.

Chancellor Angela Merkel complained to the German Parliament after learning that her cell phone records had been "monitored" by the NSA program (those of thirty-five other foreign leaders were, too, the AP reported). Her charge has been disputed by a later study, but, at the time, Merkel warned that the ethics of security in democratic states must be a model to the undemocratic states around the world.

There is a *Casablanca* element here: "There is gambling in Rick's place." Hark, nasty surveillance practices are going on! *Washington Post* columnist David Ignatius noted that the United States and Germany had cooperated for years in secret surveillance activities. NSA also works with GCHQ, its British counterpart, in surveillance practices, and the United States has arrangements with Australia, Canada, and New Zealand for sharing intelligence. Josef Joffe, the editor of *Die Zeit* in Hamburg, noted in *The Wall Street Journal* that friends do spy on friends, pointing out examples of Germany doing so, and he refers to Germany and America "as comrades-in-snooping." He added, referring to a dated adage, "This world of power, politics and