The Lessons of SHAMROCK

M. E. Bowman

The "lightning rod" in contemporary events has been the National Security Agency's Terrorist Surveillance Program (TSP). This article is not about the TSP, but it does delve into one of the chief complaints about the TSP – the privacy rights of Americans. While privacy is constantly waning due to our use of credit cards, benefits programs, and so forth, the subject is at least emotional, sometimes legal, and always political. Americans in general, and the privacy lobby in particular, cling to the notion that constitutional rights of privacy have to be carefully guarded – to which a strict constructionist not many decades past might have asked "What constitutional rights of privacy?"

It seems paradoxical to have a constitutional right not mentioned in the Constitution, but privacy has always been a whimsical topic in American culture. Even though the Constitution is silent on privacy, in 1965 the Supreme Court located a constitutional right of privacy, well outside the historical and doctrinal lineage of the Fourth Amendment, when it found unconstitutional a Connecticut statute dealing with contraceptives.[1] This may have been startling at the time, but today it seems entirely logical. For most of us, it is an article of faith that protection against intrusions by the government on the lives of the citizenry is precisely what the Bill of Rights was intended to address.

Unfocused, undefined and certainly quixotic throughout most of our history, privacy nevertheless can be traced from the founding as an essential element of our societal needs from the very beginning of the republic. However, that privacy contemplated in the early days was clearly more physical in nature than are many of the privacy rights we claim today.

In advocating the adoption of the Bill of Rights, Patrick Henry claimed that officials "may, unless the government is restrained by a bill of rights... go into your cellars and rooms, and search, ransack, and measure, everything you eat, drink, and wear."[2] In more recent years, the Supreme Court noted that "it is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment."[3] Patrick Henry did not speak of privacy directly, but rather of the evils that could be avoided if "rights" were guaranteed. Two hundred years later, the Supreme Court also focused on the evils to be avoided in order to find a right of privacy.

Probably the major reason privacy was not explicitly mentioned is that the Founders could not possibly have envisaged all the ways a future government might be able to intrude on the citizenry. In any case, privacy as we understand it today was not part of the colonial psyche. Today, however, technology provides the government, and even private individuals, the ability to be greatly intrusive in ways hardly imagined a scant few years ago. Nevertheless, recognition of the importance of privacy is often traced to an 1890 law review article, "The Right to Privacy," written by the future Supreme Court Justice, Louis Brandeis.[4] Nearly four decades later, in a dissenting view of the now discredited 1928 case, *Olmstead v. United States*,[5] Brandeis drew on principles he had first advanced in 1890 when he argued that:

> *[T]he makers of our Constitution ... sought to protect Americans in their beliefs, their thoughts.... They conferred, as against the government, the right to be let alone.... To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.*

For present purposes, the most salient point Brandeis made was that technological changes continually permit the government to employ more subtle and expansive means of invading privacy. In this, Brandeis proved to be prescient. Technologies have taken us beyond the telephone that concerned Olmstead and given us cell phones, satellite phones, e-mail, and chat, and are now moving us into virtual

1. 381 U.S. 479 (1965).

2. III The Debates in the Several Conventions on the Adoption of the Federal Constitution 448-49 (Jonathan Elliot ed., 1836).
3. Payton v. New York, 445 U.S. 573, 583 (1980).
4. Samuel Warren & Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).
5. 277 U.S. 438 (1928).

reality. Not long ago surveillance technicians were constantly frustrated when new technology had, basically, a shelf life of 90 days. An expert working in virtual reality recently commented that "it changes overnight." What does this mean for privacy? Perhaps quite a lot! If history is a bellwether, national security requirements do appear to have one constant – advancing technology consistently narrows the space between collective security and personal privacy.

Our history demonstrates an uneasy, sometimes even unstable, relationship between privacy, the Constitution and collective security. The post-World War II years are instructive for many of the issues that face us today. War gave rise to new technologies that yielded investigative and intelligence techniques that, decades later, would be scrutinized and regulated by a combination of executive, legislative and judicial guidance. One project, Operation Shamrock, initially was both modest and unassuming, but it would evolve in a way that would invite far-reaching scrutiny with lessons applicable today.[6]

Shamrock, and many other activities intended to protect the nation, illustrates that the Executive authority practiced by many presidents, and taken to logical extremes by President Roosevelt, had become a part of the landscape, not an extraordinary event authorized in time of dire peril.

Shamrock was spawned of cryptanalytic successes of the war years that had proved vital to the successful outcome of World War II.[7] At war's end, the Army Security Agency, a predecessor to the National Security Agency, sought to continue to receive foreign communications in order to maintain the cryptanalytic skills acquired in wartime. Arrangements were made with major cable companies to acquire overseas cables to, and from, foreign embassies and consulates, as well as some sent and received by U.S. persons and commercial firms. Despite advice from their attorneys that the contemplated intercept operation would be illegal in peacetime, the companies agreed to participate, provided they received the personal assurance of the attorney general of the United States that he would protect them from suit, and that efforts be immediately undertaken to legalize the intercept operation.

In 1947, representatives of the companies met with Secretary of Defense Forrestal to discuss their continued participation in Shamrock. Forrestal told them that the program was "in the highest interests of national security" and urged them to continue. The companies were told that President Truman and Attorney General Tom C. Clark approved and that they would not suffer criminal liability, at least while the current administration was in office. Those assurances were renewed in 1949, when it was again emphasized that future administrations could not be bound. There is no evidence that the companies ever sought such assurances again.

In retrospect, Shamrock, and many other activities intended to protect the nation, illustrates that the executive authority practiced by many presidents, and taken to logical extremes by President Roosevelt, had become a part of the landscape, not an extraordinary event authorized in time of dire peril.[8] Over three decades technology evolved and Shamrock evolved along with the technology. Shamrock reached its zenith when electronic media displaced paper communications.

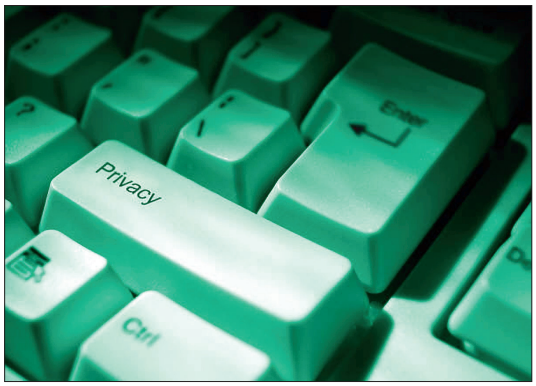
This evolution of technology was pivotal, and a turning point in both surveillance activities and future law. It was no longer necessary to hand sort paper copies of communications; computers were programmed to scan electronic media in search of words of interest. With this technological advance, "watch lists" of names were developed which soon came to be entered without reference to foreign or domestic interests. Shamrock, originally designed merely to retain skills useful in conflict devolved in a way that would doom the program, but which would also pave the way to regulation of intelligence activities. Ironically, Shamrock would go astray, at least in part, in the pursuit of justice.

As attorney general, Robert Kennedy was so taken with the possibilities of Shamrock that he employed watch lists for purely domestic purposes. Then a spin-off called Operation Minaret specifically targeted both cables and telephone calls for information about possible foreign influence on civil disturbances in the U.S. related to the Vietnam conflict. It takes little imagination to see that one program targeted domestic activity (some was allegedly, though unproved,

6. *See generally*, James Bamford, **The Puzzle Palace** 302-08, 350, 369, 372, 380-90 (1982) (describing Operation Shamrock).
7. *See id.* at 302-08.
8. A fuller examination of this phenomenon can be found in William Banks and M.E. Bowman, "Executive Authority for National Security Surveillance," *American University Law Review*, Vol. 50, Number 1, October 2000.

common crime); the other targeted First Amendment activity. Our judicial system permits fairly significant latitude for executive authority when foreign powers threaten, but it requires judicial intervention when the activity is domestic crime or the exercise of Constitutional liberties.

Consider for a moment what had happened with SHAMROCK. In the span of little more than a generation, the targeting evolved from paper copies, focused primarily on foreign missions, to electronic watch lists focused on both intelligence and non-intelligence targets. These lists included unpopular political figures, possibly criminals, and dissidents engaged in speech otherwise protected by the First Amendment. Technology had enabled an expansion of invasive activities that came under positive control only when congressional interest in intelligence activities began to focus on privacy issues. The most prominent of these congressional foci came from a Senate governmental affairs committee spearheaded by Senator Frank Church of Idaho.[9] That focus, in turn, led to both executive and legislative regulation of intelligence activities and to the law and policy that we function under today. Two distinct vectors of policy generated the privacy rights that we claim today, one social, the other legal.



PRIVACY AS A SOCIAL NEED

Several matters combined to drive the social impetus for privacy. When the nation was young, when it was at war, when it was threatened, privacy was less important than security. In a more secure environment, privacy became increasingly important. The seminal data point relevant to privacy came in 1965 when the Supreme Court, speaking through Justice Douglas found a right of privacy in the penumbras of the Constitution. In *United States v. Griswold* a constitutional challenge was flung at the State of Connecticut which had prohibited the sale of contraceptives.

The Court could easily have avoided this case. In the first place it was a contrived case, but it did technically qualify as a "case or controversy" that would satisfy the requirements for judicial intervention. Moreover, there was no obvious constitutional issue involved. The Court's intervention was legally novel, but it can also be viewed as a harbinger of what the Court is willing to do when no other organ of government can, or will, take a desired action that satisfies a significant social need.[10]

The challenge was one of privacy and, as noted above, the Constitution is wholly quiet on that subject. Nevertheless, the Court accepted the case. Part of the reason may have had to do with the decreasing fear of nuclear war and a growing social consciousness. Part no doubt had to do with a slowly dawning awareness of intrusive investigations, human experiments and mail opening conducted by the military, CIA and FBI, virtually all of which was subsequently exposed by the Church Committee. Contemporary literature of the day indicates minimal but growing awareness until the Church Committee virtually captured the headlines; but then, in the blink of an eye, both the intrusiveness of government actions and the threat to First Amendment rights became foremost in the eye of the media, and therefore of the public as well.

Two years after the *Griswold* decision the concept of a right to privacy was thoroughly tested in a criminal case, *United States v. Katz*. Reflecting on a warrantless wiretap used to convict Mr. Katz, the Court overruled and thoroughly discredited the 1928 *Olmstead* decision to hold that conversations were, indeed, subject to the requirements and prohibitions of the Fourth Amendment.

PRIVACY AS A LEGAL RIGHT

Why does SHAMROCK remain important? There are two primary reasons. The first has to do with the evolution of privacy law, driven by technology. Not until the government had the ability to be greatly

9. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities.

10. Lawyers and jurists can easily draw a parallel between the activity of the Court in Griswold and that of the Court in accepting Guantanamo detainees request(s) for Habeas Corpus in Boumediene v. Bush which granted that right. Neither case foreclosed Executive or Legislative authority, but they are remarkably alike in the sense that both serve notice that the other two branches of government had work to do.

intrusive into the private lives of the citizenry in a non-physical way was there cause to be concerned about wide-spread abuse. The Church Committee made SHAMROCK a poster child for this awareness. Since then, technology has driven increasingly sharper analysis and interpretation of the Fourth Amendment – primarily geared toward technology associated with private communications, which now are possible in a proliferating variety of media.

The second reason, simply put, is that the reasons to be intrusive are even more poignant today than they were during SHAMROCK operations and that yields a corresponding need for a legal and regulatory scheme that understands the technology. The concerns of the SHAMROCK era, the Red Menace, fifth columns, etc. were ephemeral – contemporary threats are not. Today, economic espionage, organized crime and terrorism are threats that eat at the heart of society. Organized crime threatens both global and national economies, nurtures international corruption and undermines global stability. Terrorism generates fear from uncertainty, seeks to create indiscriminate chaos and understands no humanitarian boundaries. Worse, however, we find linkages between all of these are increasing, either between parties or in adoption of another discipline's methodology. The need to prevent harm from these and other threats generates a requirement to aggressively target their actors.

Vexingly, the Bill of Rights was never intended to function as a mechanism for, or even to be a player in, issues of national security where we often see it today. In the urgency of prevention, mistakes will be made – and even a focus on actual wrongdoers can intrude on the lives of innocent bystanders in a way that can threaten the social compact. As a result, security of the nation as a whole will challenge the personal liberties that the Bill of Rights was intended to protect. The reason is simply the nature of the threats.

National security threats, such as terrorism, are unlike common crime, and often arise in the context of a bedeviling convergence of First and Fourth, and occasionally Fifth Amendment values not often present in the criminal case. In practice, this means that the probable cause requirement for obtaining surveillance authority is rarely "a fair probability that contraband or evidence of a crime will be found in a particular place."[11] That standard does not mesh well with the needs of society when the less obvious threats to the national security are at stake, and the reason Congress created the Foreign Intelligence Surveillance Court. For national security issues, probable cause must relate to status – i.e., a foreign power or an agent of a foreign power. As Justice Powell noted in what has become the seminal case for this arena, *United States v. United States District Court (Keith)*, the fundamental distinction has to do with foreign influence, not domestic crime. In practical terms, that means a focus on mental state rather than physical actions – clearly a more difficult challenge to assess than that presented by ordinary crime. Moreover, the threats are buttressed by continually improving technologies that defy the social and legal logic that made more sense in days of yore. The ephemeral nature of an actor's status, coupled with the challenges of technology that are constantly new, make it all the more important that the law play a dominant role in addressing mechanisms intended to meet these threats.

Today we have a bewildering array of new technologies that leave in the dust traditional and evolutionary thought processes of the Fourth Amendment: Wireless communications, Voice Over Internet Protocol (VOIP), steganography and multiplexed data transmissions are simply indicators of what is to come. ...virtual reality is presenting issues that confound legal thought.

The law is as much a part of our culture in this arena as is the social dimension, but technology challenges even our legal methodology. Our jurisprudence persistently drives us to make legal arguments and decisions that can fit into molds with which we are comfortable from prior experience. In the parlance of legal custom, arguments disposing of novel issues generally begin with "it is like...." With the technologies in use today, a lawyer trying to describe a new technology for legal purposes may search in vain for anything in prior jurisprudence that is "like" the technology she is trying to describe.

Today we have a bewildering array of new technologies that leave in the dust both traditional and evolutionary thought processes of the Fourth Amendment. The problems we see today are seldom "like" those we have solved in the past. Wireless communications, Voice Over Internet Protocol (VOIP), steganography[12] and multiplexed data transmissions

11. Illinois v. Gates, 462 U.S. 213, 238 (1983).
12. Steganography is hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. For example, a message might be hidden within an image by changing the least significant

are simply indicators of what is to come. Already virtual reality is presenting issues that confound legal thought.[13] To expect that the public can be protected with methodology and thought processes decades old in an environment in which computer-based technology has a stable shelf life that is increasingly diminishing is wishful thinking.

National security threats, espionage, sabotage, terrorism, etc., strike at the heart of national and individual security. These pose problems not of remediation, punishment or rehabilitation, but of the very real necessity to prevent the harm from occurring at all. More to the point, experience shows that prevention depends very heavily on the ability to conduct surreptitious surveillance and to analyze a great deal of disparate data. To do this, even the Congress, in the 2004 Intelligence Reform Bill, has noted that "In conducting the war on terrorism, the federal government may need additional power and may need to enhance the use of its existing powers."

In this climate, protection of the public will require law enforcement and intelligence officers to be intrusive in ways not previously required. The response to this should not be a knee-jerk, anti-investigative reaction. Rather, the response should be – as it was after the Church Committee – to work with the world as it exists, not as we might like it to be. Build the safeguards that meet the needs. Use technological advances not only to search out and compile information, but to protect privacy as well. In this respect, security and privacy are not mutually exclusive. We must demand that congressional and executive branch oversight mechanisms move into the twenty-first century along with the technology we will need to employ. In a prior age, these matters could be attended to at a deliberate pace. Today, the advances in technology occur so rapidly, and the threats to national security are so dire, that both the means to combat the threat and the means to ensure the greatest measure of privacy protection to individuals must develop together.

...protection of the public will require law enforcement and intelligence officers to be intrusive in ways not previously required. Use technological advances not only to search out and compile information, but to protect privacy as well. ...security and privacy are not mutually exclusive.

It takes little historical reflection to understand that our culture is one that sees national security as a process that includes societal needs. From the earliest days of the republic, the average United States citizen has considered privacy, in particular, the right to be free of government intrusion, to be an integral part of security. It is not acceptable that the government would be unable to protect its constituents, but it is also not acceptable that government intrude unchecked into the lives of the citizenry. In an age of widespread terrorism, this construct demands innovative methods of compiling and sharing information, but it also demands equally innovative methods of protecting it. SHAMROCK is, today, a crude example of the technological means to be intrusive, but it remains an important benchmark to illustrate the ease with which the use of technology can morph into activity not originally contemplated.

Technology has enhanced our lives, but it has also increased the complexity of satisfying privacy concerns while providing for collective security. Our challenge will always be to meet both demands, because both are essential capstones of American society. These are tasks we cannot shy from and they are tasks that will require some intrusions on private life – likely intrusions of a nature that we have not previously experienced. As Justice Powell wrote in the *Keith* case... "unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered."

Mr. Bowman served 27 years on active duty in the U.S. Navy, retiring in 1995 with the rank of Captain. He then served in the Senior Executive Service of the FBI, retiring in 2006. In 2007 he returned to public service and currently serves as the Deputy, National Counterintelligence Executive. The views expressed herein are not intended to represent those of the Director of National Intelligence, the Federal Bureau of Investigation or the United States Navy. Bowman also currently serves as Chairman of AFIO.

bits to be the message bits. Today we think of this as the ability to, for example, fill all the unused bits of a graphic image (such as the American Eagle) with a secret message.

13. For example, virtual reality has graphic child pornography sites, a woman claims severe trauma because her avatar was "raped" and a bank established in Second Life did not pay promised interest. At present these are issues for which our current jurisprudence has no ready answers.