Security v. Liberty

CONFLICTS BETWEEN CIVIL LIBERTIES AND NATIONAL SECURITY IN AMERICAN HISTORY

DANIEL FARBER
EDITOR

RUSSELL SAGE FOUNDATION • NEW YORK

CHAPTER 8

TECHNOLOGY, CIVIL LIBERTIES, AND NATIONAL SECURITY

PAUL M. SCHWARTZ AND RONALD D. LEE

This chapter departs in two respects from the earlier historical discussions of the dynamic between national security and civil liberties. First, the other authors focus largely on interactions among the executive branch, Congress, the judiciary, and to a lesser degree the public. By contrast, in this chapter we consider technological change and its impact on the behavior and choices of these actors. Second, a leitmotif of the preceding chapters has been the collective national response to war, insurrection, or internal threats, perceived or real. We examine the development of technology, which is increasingly driven by a highly globalized private sector rather than by the United States government. Technology itself shapes and influences the national response to war or other national security challenges. The nature of this impact on policy can, however, be difficult to parse.

We propose that, beyond the ongoing debate about the role of the three branches of the federal government in protecting civil liberties and responding to national security threats, fundamental issues exist regarding how our governing institutions should evaluate and respond to technological change. We consider the challenge of incorporating technology into the functions and processes of democratic governance.

Our particular focus is on information privacy, which concerns how public and private entities collect, process, share and store personal data. Information privacy is a key aspect of civil liberties, and one on which technology has an especially strong impact. To set the stage for the following discussion, we initially look at two topics. The first is the path by which information technology became part of the fabric of governance and society in the late 1960s. This era saw the development of bureaucratic systems of data processing. The second topic concerns the dramatic development of computing power (identified in Moore's law) and the rise of the Internet. These two developments had a significant influence on the availability and processing of personal data by both the government and the commercial sector. Indeed, the emergence of greater computer power and the Internet has meant decentralized data banks that can easily share information, and greater information sharing within and between the private and public sectors.

With this background in place, we examine technology's potential both to diminish and to enhance privacy when enlisted in the service of national security goals. We summarize and challenge the standard discourse about the relationships among technology, civil liberties, and national security. In the conventional view, there is a zero-sum game in play—technology either harms civil liberties and helps national security, or vice versa. In a sense, this zero-sum perspective is somewhat similar to the dynamic sketched in earlier chapters of this volume, in which measures taken in the name of national security diminish civil liberties. We propose that the reality regarding technology is more varied and complex than the conventional wisdom accepts, and conclude by offering observations about the challenges that technology poses for governance.

History Lessons About Information Privacy

In the 1960s, the United States government turned to electronic data processing to aid in its expanded social welfare programs, and private companies adopted computerized data processing to streamline and extend business operations. Computerization enormously increased both the volume of stored personal data and the ability of businesses and governments to analyze and extract meaning from this information.

During this period, Alan Westin and Arthur Miller wrote two landmark scholarly works that explored the emerging impact of computerized data processing on civil liberties. Both scholars recognized the emergence of technology that raised new potential threats to civil liberties. They attributed these threats to the computer's creation of novel ways to link, process, store, analyze, and transfer personal information.

In 1967, Alan Westin in his *Privacy and Freedom* surveyed a range of new technologies with special attention to "the computer-born revolution in man's capacity to process data" (158). He saw the computer as creating a new kind of "data surveillance" (366). He then argued that "as 'life-long dossiers' and interchange of information grow steadily, the possibilities increase that agencies employing computers can accomplish heretofore impossible surveillance of individuals, businesses, and groups by putting together all the now-scattered pieces of data" (366).

By 1971, four years later, the public had developed a strong interest in the topic of computers, data banks, and information privacy. One sign of this interest was the appearance that year of Arthur Miller's *The Assault on Privacy* in both a hardcover edition from the University of Michigan Press and a paperback from a popular publishing house. "Institutions of almost every description," Miller noted, "are relying on the computer to increase their data-handling capacity and to improve the efficiency of their operations" (1971, 36). He argued that the accumulation of "dossier-type material on people over a long period of time" represented a threat to "some of our most basic freedoms" (54–55).[1] This fear was based on the coming centrality of new information processing technologies; as Miller wrote, "the emerging information transfer networks can be described as society's electronic equivalent to the biological central nervous system" (273). From this perspective, the domestic intelligence-gathering and surveillance in the late 1960s and early 1970s that L. A. Powe describes in chapter 7 may well have been influenced by the availability of new technologies at the time. The question for Miller and Westin was how to regulate these new systems to preserve civil liberties in light of the new technological capabilities for surveillance. In the conclusion to *Privacy and Freedom,* Westin made two essential points:

> 1. The strict records surveillance that was for centuries the conscious trademark of European authoritarian systems . . . is now being installed in the United States . . . as an accidental by-product of electronic data processing for social-welfare and public-service ends.
> 2. There is no way to stop computerization. (1967, 326)

The new information processing systems were in fact not to be stopped. Over the subsequent years, they have made undeniably positive contributions to the effective delivery of government services and to the creation of entirely new categories of businesses. The question, still open to this day, is how best to regulate their impact on information privacy.

From the vantage point of 2008, we can see that Westin and Miller were writing at a critical juncture during which the public and private sectors were increasing their computerized data processing of personal information. In one observer's view, such early periods in the growth of technological, bureaucratic, and physical infrastructures provide critical opportunities to create the legal and social rules that will shape the resulting systems. As Thomas Hughes argued, "a technological system can be both a cause and an effect; it can shape or be shaped by society. As they grow larger and more complex, systems tend to be more shaping of society and less shaped by it" (1994, 112). The suggestion is that a critical window of regulatory opportunity may sometimes be available for each emerging technology.

As a general matter, Hughes's point is surely correct. Yet, the experience in the United States also suggests another lesson, namely, the profound instability of any legal regulation of information privacy due to ceaseless technological developments. Spiros Simitis, a leading international privacy expert, clearly pointed in 1987 to the impermanent nature of regulations in this area. Simitis noted presciently,

> No matter how precise the rules [for privacy], they nevertheless remain provisional because of the incessant advances in technology. Regulations on the collection and retrieval of personal data thus present a classic case of sunset legislation. If the legislator wants to master processing issues, she must commit herself explicitly to a constant reappraisal of the various rules. (1987, 742)

As to Simitis's view regarding the instability of information privacy regulation, technology has indeed had the kind of impact he foresaw.

Over the last three decades, the two most important technological developments in this context have been the increase in computing power as predicted by Moore's law and the rise of the Internet. Moore's law is not a legal rule, but a prediction in 1975 by a cofounder of Intel, a leading semiconductor manufacturer, regarding a continuing, steady increase in computing power per unit.[2] Time has proved Gordon Moore correct, and advances in computing power have also meant steep drops in computing costs and a creation of a wide array of new electronic devices. At the end of the 1970s, the only communication device in wide use was the landline telephone. Today, digital devices—such as computers, mobile phones, pagers, and personal digital assistants (PDAs)—create, receive, and transmit new kinds of detailed personal information, including locational information, at a speed and low cost hardly imaginable to the analog phone user of the late 1970s. The emerging technologies of radio frequency ID and transponders, such as used in the E-Z Pass on the East Coast and Fastrak in the Bay Area, also lead to the collection of personal information.

The second important technological development in recent decades has been the Internet and its widespread use across the population at large. Beginning in the 1960s, the United States Department of Defense's Advanced Research Projects Agency (ARPA) funded research into survivable communication capabilities in the case of a nuclear attack on the United States. The initial ARPANET linked computing research centers at several universities. In the 1990s, a successor network, the Internet, built on the ARPANET model and added use of the TCP/IP protocol. In the course of the 1990s, the Internet became a widespread communications medium with the emergence of the World Wide Web (WWW), based on Tim Berners-Lee's HTML format for hypertext documents.

The Internet is the most widely adopted and interoperable means to date for networking different computers—and for collecting and sharing personal information. Some computer networks have existed at least since the 1970s. In 1977, the Privacy Protection Study Commission noted the phenomenon of a "physical decentralization, but functional centralization, of records" through "computer networking—the interconnection of computers via telecommunications" (United States 1977, 9). The Internet, of course, goes considerably beyond such networks. Its openness and worldwide reach have increased the processing, combination, and transfer of personal data. It has also done so in ways that are difficult for any individual to anticipate or control.

We can develop these points by considering, first, the statute that addresses the privacy of individual videotape rental transactions, and, second, the law regarding telecommunications surveillance. The Video Privacy Protection Act was written in 1988 in such a way that it can be interpreted and applied beyond the simple corner video store to reach even online rental services, such as NetFlix, which did not exist in 1988, and to regulate rentals of DVDs, which also did not exist in 1988. So far, so good. But the statute does not address myriad issues about the application of its principles to video files downloaded, or streaming videoclips watched.

Moreover, the act of renting a video in the 1980s caused the collection of a relatively discrete amount of information. In contrast, complete information about an individual's Web surfing, video file download, and streaming videoclip viewing habits may soon be available. These data include decisions about products ordered or other action taken, and even how often specific scenes were watched and when in the day, week, and year they were viewed. This information may provide detailed insights into an individual's political and artistic preferences as well as her spontaneous self-expressive thoughts and priorities. Constitutional law considers such activities in the pursuit of self-determination as subject to fundamental protections. In these and many other areas, the rapid development and public embrace of the Internet, the digitization of content, and the widespread availability of broadband Internet connections have pushed new privacy issues to the fore at nearly breakneck speed.

As a second example, telecommunications surveillance law initially focused only on the contemporaneous surveillance of communication content. The critical statute for such surveillance is the Wiretap Act, enacted originally as Title III of the Omnibus Safe Streets and Comprehensive Crime Control Act of 1968. This statute establishes a general prohibition on law enforcement's surveillance of the content of a telephone conversation captured in "transmission," that is, in real time, in the absence of a court order (Solove, Rotenberg, and Schwartz 2006, 264–5). Today, in contrast to 1968, the thorniest questions about surveillance concern a range of telecommunications attributes considered to be less than content and to involve asynchronous communication.

Interception of information that falls into these categories is generally subject to the Stored Communications Act of 1986, which tends to offer lesser protections than the Wiretap Act. In addition, although it has been amended on numerous occasions, including by sections of the PATRIOT Act of 2001, the Stored Communications Act still largely reflects technical categories prominent when it was enacted. As Orin Kerr observes, the Act freezes "into the law the understandings of computer network use as of 1986" (2006, 502). At that time, for example, bulletin board systems were the most important kind of networked computer communications. The Stored Communications Act still refers to only two categories of network service providers: those that provide "electronic communication services" and those that provide "remote computing services" used as part of an outsourcing of tasks.

Among the difficulties that flow from these old distinctions is that at present most network service providers fulfill many functions. Hence, numerous questions under the law prove exceedingly complex. One that Kerr points to is central for the information age; it concerns "the surprising difficult case of opened e-mails" (2006, 509). Unresolved questions exist concerning the legal standard under which the government is permitted to obtain access to emails that a person has read and left with an ISP or on a remote server.

In sum, technological developments over the last three decades have both increased the ability of public and private sectors to create, combine, and compare databases of personal information and put pressure on the stability of any legislative attempts to protect civil liberties by regulating information privacy. They illustrate the difficulty of striking an enduring balance between civil liberties and government's ability to derive law enforcement and national security benefits from the use of technology.

Beyond the Standard Dichotomy

Government has also sought to harness the power of technology in the interests of national security. We now discuss the impact of technology on both national security and civil liberties. One view takes a zero-sum approach. First, technology is seen as offering a great, even unique potential for improving national security. Here, we hear the discourse of technological optimism. Drawing on the work of Leo Marx, we can define technological optimism as resting on beliefs in history as a record of progress and technological innovation as the primary agent of that progress (1994, 240). In the context of national security, moreover, technology is specifically regarded as a uniquely powerful means for safeguarding the safety of the nation.

Second, technology is also seen as raising great, even unique, dangers to civil liberties. This discourse is technological pessimism—with elements of a dystopian perspective sometimes mixed in. Technological pessimism represents a "sense of disappointment, anxiety, even menace, that the idea of 'technology' arouses in many people these days" (Marx 1994, 238). More specifically, technology is seen as creating systems of control that inexorably degrade civil liberties. In the context of privacy, the leading intellectual examples of technology gone wild are George Orwell's Telescreen from *1984* and Jeremy Bentham's Pantopicon (as rediscovered by Michel Foucault in *Discipline and Punish*). Popular culture has also sounded this theme in movies such as the *Conversation, Enemy of the State, The Matrix,* and *Minority Report.*

The standard dichotomy portrays a state of constant tension between the two sides. Technology's achievements for national security will lead to a loss for civil liberties. A gain for civil liberties will require limits on technology—and cause an attendant loss for national security. We illustrate this logic in table 8.1.

TABLE 8.1 The Standard Dichotomy

Subject Area	Overall Impact of Technology	Discourse
1. National security	Technology improves national security	Technological optimism
2. Civil liberties	Technology harms civil liberties	Technological pessimism

Source: Authors' compilation.

For a detailed example of the standard dichotomy in action, consider the public discussion and policy debate in 2002 about the Pentagon's Total Information Awareness (TIA) program. TIA was intended to revolutionize the ability of the United States to detect and counter foreign terrorists through its projected development of novel data mining and profiling techniques. This technology is made possible by the ongoing increase in computing power and the emergence of decentralized data banks in the private and public sector. TIA was led and funded by the Defense Advanced Research Projects Agency (DARPA), whose predecessor agency, ARPA, as noted, played a critical role in funding the research that helped to create the Internet. TIA's program managers stated that terrorists engaged in what TIA termed a "low-intensity/low-density form of warfare" that had "an information signature, albeit not one that our intelligence infrastructure and other government agencies are optimized to detect" (DARPA n.d.). The solution? TIA first proposed, "to fight terrorism, we need to create a new intelligence infrastructure to allow these agencies to share information and collaborate effectively." It also called for creation of "new information technology aimed at exposing terrorists and their activities and support systems" (DARPA n.d.).

Thus, TIA sought to use information technology to broaden and even automate the response to the terrorist threat. As Jeffrey Rosen summarized its research agenda, "TIA sought to develop architectures for integrating existing databases into a 'virtual centralized grand database' that would collect data from public- and private sector sources" (2004, 100). The massive TIA database was to contain information about personal finances, education, travel, health, and other areas. As Rosen observed, moreover, the database was to combine information from sources in both the private and public sectors. TIA would then apply advanced techniques and technologies to detect precursors and indicators of terrorism. In brief, TIA sought to use technology to connect the dots and allow counterterrorism officials to search different databases to identity terrorist activities.

The technological optimism behind this project was expressed in graphic form on the initial Web site for the project, quickly scuttled, which featured an eye placed on top of a pyramid and the legend *scienta est potentia* (knowledge is power). This underlying belief in the potential benefits for national security from data mining and other automated data analysis was far from limited to the TIA.

Numerous blue ribbon commissions have demonstrated a similar enthusiasm for data mining of different kinds. These groups include the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Robb-Silberman Commission), the Commission on the September 11, 2001 Terrorist Attacks on the United States (the 9/11 Commission), and the Markle Foundation Task Force on National Security in the Information Age. In the academy, Judge Richard Posner has emerged as perhaps the single greatest voice in favor of data mining (2005a, 2008). The devil is in the details, however, and questions remain regarding the safeguards necessary to protect civil liberties within any automated data analysis (Rubinstein, Lee, and Schwartz forthcoming).

The technological optimism of TIA was, however, quickly swamped by technological pessimism. An outpouring of media reports raised concerns about the implications of the program for civil liberties. A central fear regarding TIA was its combination of public and private databases. For example, *New York Times* columnist William Safire objected to the program's dismantling of "the wall between commercial snooping and secret government intrusion" ("You are a Suspect," November 14, 2002, A35).

In response to mounting public concerns, the Pentagon removed the ominous eye from the TIA Web site, changed the name of the program from Total Information Awareness to Terrorism Information Awareness, and pledged that the program would include privacy protections—although the planned privacy safeguards were left largely unspecified. In 2003, Congress voted to deny funding for TIA, though it specifically allowed funding of "processing, analysis and collaboration tools for counterterrorism foreign intelligence." Congress specified in the Defense Appropriations Act of 2004 that the results of this research were exclusively to be used in "(1) lawful military operations of the United States conducted outside the United States; or (2) lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States citizens."[3] In the discussion of TIA, much of the discourse saw the values of national security and civil liberties as inevitably in opposition.

Beyond these specific provisions in the Defense Appropriations Act of ›04, the government elsewhere has pursued TIA's goal of developing new chniques of database mining and profiling to identify terrorists. Noah ıachtman writing in *Wired* magazine in 2004, for example, identified six ›vernmental programs engaged in activities similar to those sought in IA. Of these, perhaps the best known is CAPPS II, a program to screen rline passengers by analyzing passenger records, commercial databases, ıd national security information, including terrorist watch lists. In a June ›05 report about data mining in homeland security, the Congressional esearch Service found "mission creep" to be a critical concern and found present in CAPPS II (Seifert 2005, 10). In a paper for the Center for trategic and International Studies, Mary DeRosa also raised concerns ›out mission creep in counterterrorism programs and noted the inadeuacy of current government mechanisms for controlling the use of data ıining matches (2004, vi).

Delays in the implementation of CAPPS II and concerns about its civil berties implications led to its replacement by another initiative, Secure light. This program is still in development. Thus far, the Transportation ecurity Administration has published a system of records notice, purıant to the Privacy Act of 1974 (5 U.S. Code §552a), and a privacy impact ssessment. With its privacy and processes now set out in writing, it is onducting tests of Secure Flight.

Overall, the government's technological optimism has been enduring. ıs the Pentagon's Technology and Privacy Advisory Committee (TAPAC) ›und in 2004, "TIA was not unique in its potential for data mining. 'APAC is aware of many other programs in use or under development oth with [the Department of Defense] and elsewhere in the government hat make similar uses of personal information concerning U.S. persons to .etect and deter terrorist activities" (United States 2004, viii). At the same ime, worries about the implications of technology are persistent. Thus, he standard dichotomy is well entrenched. It is also woefully incomplete.

First, depending on the context and how it is implemented, technology an protect rather than harm civil liberties. Timing is essential—acting he moment technological systems are introduced is critical. There is a reat need, for example, for legal regulation of the government's use of lata mining systems. The key challenge is to structure procedures and nstitutions for ongoing analysis of the impact of technology, positive and ıegative, on national security and civil liberties.

Second, technology may not only be a way to safeguard national secu·ity, but also to pose threats to it. We propose replacing the standard

TABLE 8.2 Technology's Multiple Impacts on National Security and Civil Liberties

Subject Area	Overall Impact	Discourse
1. National security	Technology improves national security	Technological optimism
2. National security	Technology harms national security	Technological pessimism
3. Civil liberties	Technology improves civil liberties	Technological optimism
4. Civil liberties	Technology harms civil liberties	Technological pessimism

Source: Authors' compilation.

dichotomy with an expanded analysis of technology's multiple impacts on national security and civil liberties. We present this approach initially in tabular form (see table 8.2).

In terms of this table, the standard dichotomy acknowledges only categories 1 and 4. Full analysis requires more; it calls for a look at other potential implications of technology.

Few policy analyses formally incorporate the four possibilities. More typically, scholars simply note the need for a broader analysis of technology, national security, and civil liberties. For example, in 1967, Alan Westin noted the ability of "scientific activity, especially by such groups as the telephone companies, electronics firms, and data-processing manufacturers" to "develop new systems for the protection of the average citizen's privacy" (379). This observation would fall under row 3 in table 8.2. The Privacy Protection Study Commission made a similar comment in 1977 in noting technology's failure to give "an individual the tools he needs to protect his legitimate interests in the records organizations keep about him" (United States 1977, 18). And, more recently, Jeffrey Rosen aptly called for a more complete analysis of data mining and profiling than was generally present during the TIA debate: "Nearly all [technologies of identification] can be designed in ways that strike better or worse balances between liberty and security. Depending on these design choices, the technologies can protect liberty and security at the same time, or they can threaten liberty without bringing a corresponding interest in security" (2004, 100).

Although widely overlooked in the public debate about TIA, this program at least made some attempts to harness technology to promote privacy. DARPA funded research at the Palo Alto Research Center that sought to create different automated methods to expunge from collected data the information associating that data with a specific person and to release the data only when overseen by a neutral party (that is, a federal court). This research was to incorporate civil liberty considerations into deployment of technology.

To be sure, technical and practical issues will arise and may be difficult to resolve—indeed, they may sometimes weigh against deployment of a specific technology, or counsel limits on such deployment. The conceptual ideal is to develop and deploy technology that advances both national security and civil liberties (Lee and Schwartz 2005, 1472–81). But this goal may prove elusive, and the trade-offs complex to calculate. As an example of the difficulty of the calculus, consider encryption and anonymity technologies.

On one hand, widespread availability of encryption technology might make it more difficult for the law enforcement and intelligence communities in the United States to access the plain text of terrorist communications. Technology, such as so-called onion routing, which allows anonymous communications and communication paths, can also assist terrorists. On the other hand, strong cryptography prevents terrorists and criminals from violating the privacy of others and helps to keep our critical digital infrastructure secure. Moreover, onion routing has already been used by a U.S. Navy unit to disguise its communication patterns. The benefit to the government of a public anonymizing network is that "a widely used anonymity system provides Department of Defense users the best protection from prying eyes" (Diffie and Landau 2007, 274). As the developers of Tor, the most current version of onion routing, have stated, "anonymity loves company" (Dingledine and Mathewson 2005, 547).

We turn now to row 2 of table 8.2, which concerns the harms that technology can visit on national security. From the perspective of 2008, there are three distinct developments related to technology that have enormously increased the potential harm to national security. Just as this chapter has traced history lessons about the impact of technology upon information privacy, an element of civil liberties, it is also possible to consider the impact of technology on national security. These historical lessons are not cheerful ones.

First, technology has increased the destructiveness of the weapons at the disposal of America's adversaries; these include a wide range of weapons of mass destruction, including nuclear, radiological, biological, chemical weapons, as well as more conventional ones. These weapons greatly increase the potential for harm to our society—especially in the hands of nonstate actors that hold extreme views and are less susceptible than nation-states to the conventional military, diplomatic, economic, legal and moral pressures that other nation-states can bring to bear.

Second, the United States and many other nations targeted by terrorist groups are highly industrialized and depend heavily on technology, opening the door for asymmetrical warfare to be waged against them. Terrorists have misappropriated the advanced technology of a nation to cause great damage and harm at low cost to them. On September 11, 2001, terrorists armed with box cutters hijacked commercial aircraft fully fueled for transcontinental flights and turned them into large-scale lethal weapons. The 9/11 Commission estimated the planning and execution costs of the attacks at between $400,000 and $500,000 (169). The operation caused inestimable human loss and suffering, as well as billions of dollars in harm to the American economy as well. The New York City comptroller estimated the cost to New York City alone as between $83 billion and $95 billion (Thompson 2002).

Beyond dangers to the United States' air passenger transportation system, the United States faces other risks to the safety of its nuclear plants, its telecommunications and financial systems, and its transportation infrastructure of trains, subways, highways, and ports. The possibility of bioterrorism places new demands on the public health surveillance and response system. The possibility of cyberterrorism poses a threat to the Internet and other communication networks.

Finally, technology empowers terrorists by allowing them to recruit new members and supporters, and to fund their activities more readily, across greater distances, and within shorter time frames. It also allows terrorists to communicate, coordinate, and conceal their operations. The Internet and digital technologies, for example, allow nearly instantaneous, low-cost international communications. In an illustration of this point, as reported in the *New York Times*, in July 2007, Prime Minister Gordon Brown offered the British House of Commons the following tally of the devices and data involved in a terrorist plot against transatlantic airliners that British intelligence had foiled the previous year: 200 cellphones, 400 computers, and 8,000 CDs, DVDs and discs containing 6,000 gigabytes of data (Jane Perlez, "British Leader Seeks New Terrorism Laws," July 26, 2007, A8).

The vast data cloud of world and domestic communications may also increase the difficulties posed for governments in developing accurate and timely intelligence about the intentions and plans of terrorists. In apparent response to these difficulties, President George W. Bush acknowledged in 2005 that he had authorized the National Security Agency "to intercept the international communications of people with known links to al Qaeda and related terrorist organizations" where one end of the communication was outside the United States. The administration asserted that required procedures under the Foreign Intelligence Surveillance Act did not provide for the requisite speed and agility. These administration claims have proved controversial. Nonetheless, sustained attention by legislators, policy makers and an informed citizenry is especially needed for issues at the intersection of technology, civil liberties, and terrorism.

Historical Discontinuities, Historical Continuities

We close with exploration of a larger question, which is whether (or not) technology has wrought a fundamental change in the historical relationship between civil liberties and national security. In large part, the preceding chapters describe a dynamic in which a public security threat disrupts a balance between civil liberties and national security. The new threat triggers political and public responses. The executive branch plays an especially prominent role, and the judiciary, the Congress, and the public may agree, disagree, or simply acquiesce. Over time, a backlash or reaction to new policies emerges, as the underlying threat is eliminated or perceptions about the magnitude of the threat change. Ultimately, a new balance is achieved.

By contrast, other chapters of this book note that this dynamic may prove different in confronting radical international terrorism because of the potential for this threat to persist without the possibility of a clear and declarable victory by the United States and its allies. There is also another reason for thinking that the dynamic may evolve differently this time; technology may upset the pace and outcome of this traditional ebb and flow. To the extent that it does, this chapter points to a different lesson than the rest of this book.

There are two ways that technology might affect the traditional fashion of reaching a new equilibrium. First, the rapidity by which technology generates new policy issues may mean that any balance between civil liberties and national security is inherently evanescent. A new equilibrium requires agreement among the three branches of government and the governed, stasis among particular technologies or technological capabilities, and consensus about the application of agreed legal principles to the new situation.

Second, the government has traditionally played a central role, sometimes for better and sometimes for worse, in the civil liberties and national security dynamic. The private sector's important role in developing and commercializing technology may lessen the government's ability to preside over the civil liberties and national security dynamic. This impact may be particularly drastic because the private sector driving technological change is inherently global and transnational in its workforce, sources of innovation, economic interdependencies, and market focus.

IMPERMANENCE

In *Perilous Times,* Geoffrey Stone draws a central lesson from the history of major restrictions of civil liberties in the past. Looking at events of 1798, 1861, 1917, 1942, 1950 and 1969, he comments that historical differences in suppression of dissent depend heavily on "the extent to which national political leaders intentionally inflamed public fear" (2004, 533). Moreover, "again and again, Americans have allowed fear to get the better of them" (529). For Stone, "the unimpeachable lesson of history" is that the government has established a pattern of overreaction, leading to excessive wartime repression of civil liberties, and, in particular, freedom of speech (530). In chapter 5 of this volume, Stone ends with an analysis of *Hamdan v. Rumsfeld* and a suggestion that the Supreme Court may be about to engage in more aggressive protection of individual rights.

In *Uncertain Shield,* Richard Posner disagrees with Stone's conclusion. He points to a "continuing ominous evolution in the availability and lethality of the technologies of destruction" and, striking a different note, worries "about the prospects for sound organizational reform" of the American intelligence community (2006, xx–xxi, 211). Like Stone, however, he sketches a process in which civil liberties rebound over time and a new equilibrium is established (2005b, 186–9; 192–7). Similarly, Alan Brinkley in chapter 2 of this volume describes how the reaction to repression of civil liberties in the United States during World War I led Justices Brandeis and Holmes and other members of the Supreme Court to create "the legal and moral basis for our modern concept of civil liberties." For Stone, Posner, and Brinkley, there is a general tendency over time toward equilibrium in the balance between civil liberties and national security interests.

Yet, the history of technology, data processing, and information privacy we have explored here teaches the impermanence of legal regulation and the insistent challenges by technology to existing balances. Nothing has been so constant in this area as change. Sic transit gloria mundi. Another argument about the constancy of change, from a different perspective, is made by Jan Lewis in chapter 6 of this volume. She discusses how the American identity has always been a work in progress, and proposes that in America "citizenship is always contested" and civil liberties "never wholly secure."

The Government's Role

In the past, the government has been a dominant player in the dynamic involving civil liberties and national security. Consider its role in adopting and enforcing the Alien and Sedition Acts, the suspension of the writ of habeas corpus during the Civil War, the Espionage Act in 1917, the Sedition Act in 1918, the Palmer raids, the internment of Japanese Americans during World War II, McCarthyism, and the domestic surveillance activities of the intelligence community in the 1970s that led to the enactment of the Foreign Intelligence Surveillance Act.

Technology appears to have changed the ability of government to exercise a central role. The greater power of the private sector in developing technology and the greater disruptive effects of technology, as in asymmetrical warfare, are among the factors that have weakened the power of the government. Nonetheless, the government will continue to have an important role, indeed a unique role, in protecting national security and safeguarding civil liberties.

We conclude by pointing to the concept of public liberty that Stephen Holmes develops in the final chapter of this volume. For Holmes, a concept of public liberty is needed in the current debate about the liberty-security tradeoff. Holmes makes an important distinction between "the private liberty of private individuals to behave as they choose so long as they refrain from harming each other" and "the public liberty of citizens to examine and criticize their government, and to strive to out it from power in competitive elections, so long as they obey the law." Public liberty allows citizens to compel government to give reasons for its action. It serves to improve security by preventing policy makers from hiding their errors from the public view and avoiding criticism. As Holmes proposes, "the aim of liberal institutions should be to facilitate the psychologically painful process of recognizing past blunders and initiating requisite mainstream readjustments."

Whether in dealing with new technologies or with new threats to national security, the health of a democratic system depends on an informed citizenry willing to participate in civic affairs. A public discussion about important technological issues, such as data mining or the impact of technological advances on existing statutory frameworks regulating electronic surveillance, would be an important exercise of Holmesian public liberty. Indeed, there is an emerging agreement among at least some policy experts regarding the necessary regulation of data mining (Rubinstein, Lee, and Schwartz forthcoming). As part of this regulation, there must be public debate about the reliability and track record of both government and commercial data mining, and the makeup and operation of data mining systems. Some residue of information may necessarily be kept secret for national security reasons. Nonetheless, public release of information and public debate are needed for the design, performance, and privacy protections in data mining systems.

Conclusion

This chapter first considered the history of computerized processing of personal information in the United States. There was no stopping the adoption of electronic data processing by the public and private sectors; the question has been how to regulate the processing of personal data to protect information privacy while realizing the value of computerized data processing for both government and private sector endeavors. The chief lesson of the confrontation of United States law with widespread adoption of electronic data processing has been the instability of legal regulation for information privacy.

We have questioned the conventional wisdom in which technology's benefits for national security are viewed as coming at the cost of civil liberties, and vice versa. In a more complete view, technology can also harm national security, and it can benefit civil liberties. Substantial governmental and public attention is needed to manage the consequences of technology's disruptive effects. Having explored a series of historical discontinuities and historical continuities, we wonder if technology has disrupted the traditional and recurring processes in which civil liberties and national security values have been balanced in the United States. Public liberty, without question, requires increased public discussion and debate about the role of technology and the regulation of technology in shaping and reshaping the dynamic balance between civil liberties and national security.

Notes

[1] Miller also observed, "many people have voiced concern that the computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been stored in it, may become the heart of a surveillance system that will turn society into a transparent world in

which our homes, our finances, and our associations will be bared to a wide range of casual observers, including the morbidly curious and the maliciously or commercially intrusive" (1971, 16).

2. In a popular formulation of Moore's law, the prediction is that the number of transistors, and hence the available processing power, that can be placed on a given size of integrated circuits will double every eighteen months.
3. Pub. L. No. 108-87, 117 Stat. 1102 (September 30, 2003).

References

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction [Robb-Silberman Commission]. 2005. *Report to the President of the United States.* Washington: Government Printing Office. Accessed at www.gpoaccess.gov/wmd/pdf/full_wmd_report.pdf.

DARPA. No date. Information Awareness Office home page. Accessed at http://infowar.net/tia/www.darpa.mil/iao.

DeRosa, Mary. 2004. *Data Mining and Data Analysis for Counterterrorism.* Washington: Center for Strategic and International Studies.

Diffie, Whitfield, and Susan Landau. 2007. *Privacy on the Line,* updated and expanded edition. Cambridge, Mass.: The MIT Press.

Dingledine, Roger, and Nick Mathewson. 2005. "Anonymity Loves Company." In *Security and Usability: Designing Secure Systems that People Can Use,* edited by Lorne Faith Cranor and Simson Garfinkel. Sebastopol, Calif.: O'Reilly Media.

Hughes, Thomas P. 1994. "Technological Momentum" In *Does Technology Drive History: The Dilemma of Technological Determinism,* edited by Merritt Roe Smith and Leo Marx. Cambridge, Mass.: The MIT Press.

Kerr, Orin. 2006. *Computer Crime Law.* St. Paul, Minn.: West Publishing.

Lee, Ronald D., and Paul M. Schwartz. 2005. "Heymann: Terrorism, Freedom and Security: Winning Without War." *Michigan Law Review* 103(6): 1446–82.

The Markle Foundation. 2003. *Creating a Trusted Information Network for Homeland Security.* Second Report of the Markle Foundation Taskforce. New York and Washington: Markle Foundation.

Marx, Leo. 1994. "The Idea of 'Technology' and Postmodern Pessimism." In *Does Technology Drive History: The Dilemma of Technological Determinism,* edited by Merritt Roe Smith and Leo Marx. Cambridge, Mass.: The MIT Press.

Miller, Arthur R. 1971. *The Assault on Privacy: Computers, Data Banks, and Dossiers.* Ann Arbor, Mich.: University of Michigan Press.

National Commission on Terrorist Attacks Upon the United States [The 9/11 Commission]. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States.* New York: W. W. Norton.

Posner, Richard A. 2005a. "Our Domestic Intelligence Crisis." *Washington Post,* December 21, 2005: A31.

———. 2005b. *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11.* Lanham, Md.: Rowman and Littlefield.

———. 2006. *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform.* Lanham, Md.: Rowman and Littlefield.

———. 2008. "Privacy, Surveillance, and Law." *University of Chicago Law Review* 74(5). Forthcoming.

Rosen, Jeffrey. 2004. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age.* New York: Random House.

Rubinstein, Ira S., Ronald D. Lee, and Paul M. Schwartz. Forthcoming. "Data Mining and Internet Profiling." *University of Chicago Law Review* 75.

Seifert, Jeffrey W. 2005. "Data Mining: An Overview." CRS Report #RL31798. Washington: The Library of Congress, Congressional Research Service.

Shachtman, Noah. 2004. "Start: Homeland Security—The Bastard Children of Total Information Awareness." *Wired* 12(2). Accessed at http://wired.com/wired/archive/12.02/start.html?pg=4.

Simitis, Spiros. 1987. "Reviewing Privacy in an Information Society." *University of Pennsylvania Law Review* 135(3): 707–46.

Solove, Daniel J., Marc Rotenberg, and Paul M. Schwartz. 2006. *Information Privacy Law*, 2nd edition. New York: Aspen Publishers.

Stone, Geoffrey R. 2004. *Perilous Times: Free Speech in Wartime: From the Sedition Act of 1798 to the War on Terrorism.* New York: W. W. Norton.

Thompson, William C. 2002. "Thompson Releases Report on Fiscal Impact of 9/11 on New York City." Press release PR02-09-054, September 4, 2002. New York: NYC Comptroller, Press Office. Accessed at http://www.comptroller.nyc.gov/press/2002_releases/02-09-054.shtm.

United States. 1977. "Technology and Privacy: Appendix 5." In *Final Report of the Privacy Protection Study Commission Joint Hearing Before the Committee on Governmental Affairs, United States Senate, and a Subcommittee of the Committee on Government Operations, House of Representatives.* 95th Cong., 1st Sess. (July 12, 1977). Washington: Government Printing Office.

———. 2004. *Safeguarding Privacy in the Fight Against Terrorism: The Report of the Technology and Privacy Advisory Committee for Secretary of Defense Donald Rumsfeld.* Washington: Technology and Privacy Advisory Commission. Accessed at http://purl.access.gpo.gov/GPO/LPS52114.

Westin, Alan F. 1967. *Privacy and Freedom.* New York: Athenum.