Securing the Virtual State: Recent Developments in Privacy and Security
G. David Garson

Social Science Computer Review 2006 24: 489
DOI: 10.1177/0894439306289100

The online version of this article can be found at:
http://ssc.sagepub.com/content/24/4/489

Published by:
SAGE
http://www.sagepublications.com

Additional services and information for Social Science Computer Review can be found at:

Email Alerts: http://ssc.sagepub.com/cgi/alerts

Subscriptions: http://ssc.sagepub.com/subscriptions

Reprints: http://www.sagepub.com/journalsReprints.nav

Permissions: http://www.sagepub.com/journalsPermissions.nav

Citations: http://ssc.sagepub.com/content/24/4/489.refs.html

>> Version of Record - Oct 17, 2006

What is This?
Securing the Virtual State
Recent Developments in Privacy and Security

G. David Garson
North Carolina State University, Raleigh

Recent developments in U.S. privacy and security policy are traced, including coverage of the renewal of the PATRIOT Act, the domestic spying affair of 2005 to 2006, passage of the Real ID Act, and other developments associated with the Department of Homeland Security. Threats to democratic values are assessed.

Keywords: privacy policy; information security; PATRIOT Act; Real ID Act; Department of Homeland Security; Bush administration information policy

As has been widely reported, information security rose to first place priority after 9/11. The FY 2005 Office of Management and Budget (OMB) report on agency compliance with the Federal Information Security Management Act of 2002 found that the percentage of systems certified and accredited as meeting security standards had risen to 85%, an increase over 77% in FY 2004 (Dizard, 2006b). Such improvements in information technology (IT) security are attributed to efforts mobilized by the Y2K problem of 2000 and terrorist attacks on September 11, 2001, and to the subsequent emphasis given to security by the Chief Information Officers (CIO) Council and in IT budgets in the 2001 to 2006 period. With investment in a presumably more information-secure state, these questions may be asked: What have we bought with our money? Is it the same kind of state we have appreciated for so many years, or are we changing it into something different from what we have known?

There is no doubt that we have mandated IT security at unprecedented levels. As of September 30, 2005, the Federal Acquisition Regulations Council has required federal agencies to incorporate IT security in all purchases, including conforming to agency-specific security requirements, and to consult security specialists when making IT purchases (Miller, 2005; Vijayan, 2005). This implemented the Federal Information Security Management Act of 2002 (part of the E-Government Act of 2002), which called for heightened security throughout system life cycles. Similarly, at the state level, the Department of Homeland Security’s (DHS) FY 2006 grant application kit for competition for $3.9 billion in IT funds urged states to conform to new 2005 national standards for the National Information Exchange Model, an XML-based model for information sharing. Although cybersecurity planning had been encouraged previously, for FY 2006 for the first time, states and localities seeking grant funds were called on to develop and implement a comprehensive cybersecurity plan and establish an information security officer as a 24-7 point of contact. Using the carrot of the $2.5 billion State Homeland Security Grant Program and
the $862 million Urban Area Security Initiative, DHS set forth numerous additional specific security guidelines for states and localities (Lipowicz, 2006b).

Renewal of the PATRIOT Act, 2006

The legislation providing the overarching framework for security is, of course, the PATRIOT Act, which was renewed recently. In mid-December 2005, the Senate rejected the reauthorization of the PATRIOT Act by a vote of 52 to 47, with opposition coming largely on privacy rights grounds. A week later, a 5-week extension was granted, and then on February 2, 2006, another 5-week extension was approved by Congress. Finally, on March 2, 2006, the Senate passed a modified version of the renewal act by a vote of 89 to 10. Fourteen of 16 PATRIOT Act provisions were made permanent, with 2 others (including roving wiretaps) given a renewal for 4 years. In spite of the widespread general attention to civil liberties issues, few Americans or even social scientists have given attention to the details of the renewal.

Particularly controversial was Section 605 of the House version of the PATRIOT Act renewal, which created a permanent national police force under the Secret Service with the power to make arrests without warrant for any offense against the United States committed in their presence or for any felony under the laws of the United States. Although the Secret Service had already exercised such powers in the District of Columbia, Section 605 nationalized the scope of a secret police force with powers of warrantless arrest. The renewal of the PATRIOT Act made Section 605 permanent.

Other controversial aspects of PATRIOT Act renewal included:

- “Sneak and peek” searches, which are physical searches of homes and offices without notice, before or after, that privacy was being invaded. At issue was whether such searches would have to be followed by notice 7 or 30 days after the search. The renewal bill continued sneak and peak searches and provided for 30-day notification, but law enforcement appeals could extend notification indefinitely.
- Roving wiretaps of selected premises were provided. At issue was whether enforcement authorities would have to determine that a specific target was probably present before surveillance was initiated. The renewal bill extended roving wiretaps for 4 more years.
- PATRIOT Act Section 215 authorized the FBI to take out secret court orders forcing businesses and organizations to disclose personal records (e.g., library records, Internet service provider records, bank records). At issue was whether the FBI should be required to show a connection between the records and suspected terrorism. The renewal bill imposed no such requirement but renews Section 215 for only 4 years.
- Section 215 also criminalized the disclosure by librarians, Internet service providers, or others of searches of their records. At issue was whether organizations should have a right to inform their members, clients, or customers that their privacy had been violated. The renewal as passed extended the gag order for 1 year, after which it gave subpoena recipients in terrorist investigations the right to challenge in court the requirement that they refrain from telling anyone. As few libraries or other subpoena recipients would be willing to undertake an expensive court fight with the government, which would claim secrecy was required by national security, critics called this concession to civil liberties merely “cosmetic.”
Between passage of the PATRIOT Act in 2001 and 2005, more than 30,000 National Security Letters (NSLs) were issued by the FBI, forcing businesses and organizations to turn over records. At issue was whether the current requirement of relevance needed to be tightened to restrict wholesale use of NSLs. One proposal was to require NSLs to be approved by the FISA Court or a federal judge. The renewal continued NSLs but did stipulate that libraries could not be recipients of NSLs unless they ran Internet servers and that the FBI could not demand the name of a lawyer consulted about a NSL, as had been the practice. The renewal law made explicit that judicial review of NSLs is allowable.

Also at issue was a proposal to make disclosure of an NSL a crime with a 5-year jail term if there was intent to obstruct an investigation (in the view of enforcement authorities, not in the view of the organization). The renewal bill retained NSL disclosure penalties. The renewal law also provided that nondisclosure orders were no longer to attach to NSL requests on an automatic basis.

At issue was whether organizations would have the right to appeal Section 215 and NSL records search requests and, if so, whether the appeal process would be pro forma or meaningful. The renewal bill did provide for individuals receiving Section 215 orders to seek judicial review. The renewal bill supported the right of NSL recipients to seek legal counsel but did not spell out any appeal rights apart from appealing gag orders.

The PATRIOT Act employs a vague and expansive definition of terrorism, to include a broad range of political activities. Domestic terrorism is defined to include acts “dangerous to human life” in violation of criminal law, if the act involves intimidation or coercion of a civilian population, influence of government policy by intimidation or coercion, or affecting the conduct of government through mass destruction, assassination, or kidnapping. The ACLU (2002) has noted that Greenpeace, Operation Rescue, Vieques Island, and World Trade Organization protesters and the Environmental Liberation Front had all engaged in activities that could subject them to being investigated as engaging in domestic terrorism. The renewal act did not alter the definition of terrorism.

The PATRIOT Act allowed information gathered in warrantless searches to be used in criminal trials, where such information would otherwise be inadmissible as having been illegally obtained. The renewal act left this intact.

In summary, in the PATRIOT Act renewal, the Bush administration pushed for permanent expansion of relatively unrestricted police powers in the name of antiterrorism but faced opposition from Democrats, joined by libertarian Republicans, opposed to conferring further police state powers on the president (“Congress Extends,” 2006). In the end, however, the PATRIOT Act was renewed with expansive executive powers for domestic spying, with most areas of controversy resolved in favor of executive power at the expense of civil liberties.

The Domestic Spying Affair of 2005 to 2006

When security powers are increased, as with the PATRIOT Act renewal, public trust rests on the credibility of officials with respect to the use of their powers. This credibility was challenged when, just before Christmas 2005, the New York Times revealed that after the 9/11 terrorist attacks in 2001, President Bush had authorized the National Security Administration (NSA) to intercept telephone calls and e-mail traffic without the benefit of court-issued warrants. The Bush administration defended its action on the grounds of
homeland security and the need to pursue its antiterrorist efforts. As authority, Bush cited his presidential powers as commander in chief, his inherent powers to act to protect the American people, and Congress’s post-9/11 resolution authorizing him to wage war on terrorists. The administration at first claimed that spying was limited to calls or e-mails in which at least one end of the communication was in another country but later admitted that domestic-to-domestic traffic had also been surveilled, allegedly “by accident.” The president’s attorney general, NSA advisor, and other administration officials rallied behind the president (Lichtblau, 2006).

The issue of domestic spying immediately became front-page news, with some Democrats calling for creation of an independent counsel to investigate possible violation of the Fourth Amendment’s prohibition against unreasonable searches and seizures—the constitutional provision on which is the basis for the requirement for court authorization of warrants and wiretaps. The warrantless electronic surveillance program of the Bush administration had bypassed court approvals, even after-the-fact ones, even by the secretive Foreign Intelligence Surveillance Court (FISC, established in the 1970s under the Foreign Intelligence Surveillance Act). The PATRIOT Act had designated FISC as the only court authorized to issue surveillance orders in investigations of terrorism, and it was thought to approve almost all requests submitted to it.

Domestic spying seemed to be part of a general policy, not an aberration, because also in December 2005, the ACLU had released new FBI records (released as a result of a lawsuit over FBI activities in relation to the 2004 national political conventions) showing ongoing monitoring of antiwar, civil rights, environmental, and other activist groups. “Our government is spying on Americans—unapologetically, unnecessarily and with no regard for the Constitution,” the ACLU stated (Fisher, 2005).

Although Congressional leaders, including Democrats, had been briefed about the domestic spying program, the briefings had bound them to secrecy, precluding even obtaining legal opinions regarding the constitutionality of the program. When the issue became public, various Senators made known that they had sent Vice President Cheney letters raising legal issues, but with no response. The no-discussions policy was further emphasized when, immediately after the domestic spying affair became public, the Bush Justice Department moved to investigate and prosecute the whistle-blowers who had leaked the story.

**Privacy Protection in the Age of Homeland Security**

On the administrative side, the DHS is a major recipient of increased IT security powers and funds. Special issues of privacy have surrounded the DHS since its inception. Under criticism from civil libertarians fearing the escalation of intrusions into individual privacy based on the PATRIOT Act and other legislation, Congress created a DHS Privacy Office at the same time that it created the DHS itself in 2002. Although the Privacy Office won praise for its reports critical of privacy protections under the Transportation Security Department’s Computer-Assisted Passenger Prescreening System, civil liberties advocates have continued to charge that the DHS Privacy Office has too little authority to compel cooperation in investigating privacy complaints, relying instead on voluntary compliance. Moreover, because the Privacy Office must clear reports through the DHS secretary, civil libertarians fear the possibility of political stifling of critical reports in the future. In 2005,
Rep. Bennie Thompson (D-Miss.) introduced the “Power Act” to give subpoena powers to the DHS Privacy Office and otherwise enhance its independence (Lipowicz, 2005a), but such reforms have gone nowhere.

Perhaps in response to criticism regarding its information security policies, the Bush administration in 2005 added privacy to the quarterly President’s Management Agenda scorecard, which rates agencies from red (worst) to yellow to green (best) on a variety of criteria. As of the end of 2005, only 9 of 26 agencies were found to conduct privacy impact assessments for at least 90% of their major IT systems (Mosquera, 2005). Moreover, in the past, privacy impact assessments have focused on procedural rather than substantive privacy, leaving civil libertarians unsatisfied.

In February 2005, the OMB issued a memorandum requiring all federal departments and agencies to designate “the senior official who has the overall agency-wide responsibility for information privacy issues” (OMB, 2005). The OMB noted that consistent with the Paperwork Reduction Act of 1995, the agency’s chief information officer could perform this role. The controversy, of course, was that the CIO also was responsible for information access, security, and other matters that could conflict with privacy goals and thus suffered conflict of interest. The OMB memo fell short of requiring separate, let alone independent, privacy officers in each department. Moreover, a 1998 memorandum (OMB, 1998) had earlier required designation of departmental privacy officers and the conducting of privacy reviews, and the issuing of the 2005 memo was a tacit admission that there were shortcomings in implementation of the Privacy Act of 1974, the Computer Matching and Privacy Protection Act of 1988, the Paperwork Reduction Act of 1995, and the Commerce Department’s Principles for Providing and Using Personal Information (“Privacy Principles”), published by the Information Infra-structure Task Force in June 1995.

**Administrative Problems of the DHS**

A prime mandate of the DHS is data integration. Toward this goal, in 2002, in the aftermath of the 9/11 terrorist attack on New York and Washington, D.C., the Joint Regional Information Exchange System (JRIES) was formed, eventually falling under the aegis of the DHS. Its purpose was to create a national antiterrorism information-sharing network linking police intelligence units and serving as a vehicle for sharing daily antiterrorism information among federal, state, and local officials. However, in 2005 negotiations over JRIES broke down, with major city police intelligence directors terminating full integration with the Homeland Security Information Network (HSIN) because DHS wished to include non-law-enforcement officials (e.g., state homeland security advisors) in the network, although police wished sensitive information to be restricted to law enforcement officials, if only for legal reason (Lipowicz, 2005c). Currently, police share much information with HSIN but have been seeking funding for their own separate network for sensitive information.

Community officials have complained that security intelligence via HSIN has been slow to come, and when it does come, it lacks useful detail (McKay, 2005, p. 34). Partly in response to such criticisms, the DHS reorganized in 2005, under the direction of Michael Chertoff, the new DHS secretary, creating a new Office of Intelligence and Analysis and revising the Homeland Security Advisory System. Chertoff made better sharing of information with state and local government one of his six top priorities. HSIN data sharing comes via the
HSIN-Secret network, which Chertoff has acknowledged already is accessible by “tens of thousands of users” (DHS, 2006). That is, inherent in the DHS information systems design is the integration of massive personal databases, in part drawing on information from the PATRIOT Act and other unprecedented increases in police powers, then allowing a pre-cleared, extremely large group of users to access it. The question is, Is abuse inevitable under such a design? Unfortunately, the cloak of secrecy may keep the answer to this question hidden for some time.

In early 2006, the inspector general for the DHS reported a variety of shortcomings with DHS’s web security. Though DHS monitored computers on its web, monitoring did not necessarily result in management action. One problem was volume, with 65 million security alerts in a 3-month study period. A greater problem was that DHS’s automated security tools could not identify specific workstations which generated the messages. Also, the security alert messages, such as “detect.misuse.porn” did not necessarily indicate what they purported (e.g., nonpornography traffic could generate the pornography warnings, which were 10% of all security warnings) but instead were triggered by use of such words as oral (Lipowicz, 2005c). The inspector general’s audit also found DHS lacked security accreditations and certifications, compliance with which it expected of others. The security and other DHS IT failures were blamed by the inspector general in part on the fact that the CIO reports in a relatively low position in the DHS hierarchy, with only 50 of 5,000 IT professionals reporting to him (Chabrow, 2005).

In addition to problems with data integration and web security, the IT track record of DHS in managing its own affairs is also problematic. In January 2006, the DHS cancelled its contract with BearingPoint, Inc., for the Emerge2 comprehensive management system (Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency 2), in spite of having invested $9 million in the $229 million contract (Temin, 2006). The abandonment of Emerge2 was a tacit admission of failure in its one-size-fits-all enterprise software approach to financial systems. DHS instead opted to allow its diverse constituent agencies to choose from among an array of existing public and private sector financial services providers, hoping later to be able to pool the data from these different providers in a way that still supports data warehousing for purposes of central reporting and data analysis. The Emerge2 name was continued, but now with what DHS optimistically called a heterogenous “centers of excellence” strategy (Dizard, 2006a). DHS claimed the $9 million was not wasted but was well spent as it resulted in clarifying requirements and training plans and a web portal to be used by DHS financial managers. Although some hailed DHS’s action for catching a probable megafailure early on, both the Emerge2 program manager and the DHS chief financial officer quit in late 2005 or early 2006, leaving the task of creating a DHS financial management system to others. At this writing, DHS has yet to prove that it is up to the IT mandates under which it was created half a decade ago.

Toward a National ID System

The United States is moving rapidly toward a de facto national ID system, something once associated with autocratic regimes such as apartheid-era South Africa. In this, the United States is not at all alone. Belgium, for instance, was the first European Union country to issue national ID cards to its citizens, with 1 million cards in circulation in 2005,
expected to rise to more than 8 million by 2009. The cards are used for both public and private sector authentication, including online tax transactions, document requests, library loans, and access to local services such as swimming pools and private sector transactions such as ticket purchases (Government Technology News Staff, 2005).

Bush- and Republican-sponsored, the Real ID Act of 2005 passed mostly along party lines and largely without debate in Congress or much attention from the media. It was embedded in an emergency military appropriations bill for Iraq to make it hard for opponents to vote against it. Its stated purpose is “to establish and rapidly implement regulations for State driver’s license and identification document security standards.” The Real ID Act compels states to design their driver’s licenses by 2008 to comply with federal antiterrorist standards. Federal employees would then reject licenses or identity cards that do not comply, which could curb Americans’ access to airplanes, national parks, federal courthouses, Social Security, even bank accounts. It will take effect in 2008.

Under the Real ID Act, DHS is given authority to specify standards, which could include biometrics (fingerprints, iris scans), radio frequency identification tags, and DNA information. It will include basic identity information and a digital photo. State departments of motor vehicles will have to require much more identification than in the past. (Another unfunded mandate to the states.) Departments of motor vehicles will require most license applicants to show a photo ID, a birth certificate, proof of their Social Security number and a document showing their full name and address. All of the documents then would have to be checked against federal databases.

The Real ID Act probably will involve creation of a massive national database on individuals, though there is still a chance the Real ID cards will only be checked locally on an individual basis (e.g., Does the cardholder have the fingerprints the card says he or she has?). Whether there will be such a database and who will have access to it, including commercial access, has not been determined.

**Summary**

Although e-government is often advertised in terms of advancing democracy and civic participation, the dark side is that it may also involve threats to democratic values such as personal privacy. When e-government is part of a large effort to secure the state, using IT as a major part of security strategy, earnest efforts may focus on technical achievements that run roughshod over such values, creating a democratic backlash. This happened in South Korea’s attempt to implement an electronic education system and electronic national IDs, precipitating fierce popular opposition led by the Korean Teachers’ Union and others who denounced e-government initiatives as threats to privacy and who were able to deal e-government implementation a major setback as a result (Jho, 2005). Thus far in the United States, there has been no similar popular reaction against trends outlined in this article. However, social science theory suggests that in the long run, the success of any institutional effort, including the building of a secure virtual state, rests on its conformity with the fundamental values of the culture in which it is found. Presumably, privacy and democracy remain core values of American political culture. This fact provides a cautionary flag to those who think that the pendulum that has brought information security to the highest priority may not in the predictable future swing back toward other priorities of our democratic culture.
References


G. David Garson is a professor in the Public Administration Program of North Carolina State University. He is editor of the Social Science Computer Review, and his most recent book is Public Information Technology and E-Governance: Managing the Virtual State (2006). He may be contacted at david_garson@ncsu.edu.