Preface

It behooves every man who values liberty of conscience for himself, to resist invasions of it in the case of others: or their case may, by change of circumstances, become his own.

Thomas Jefferson (1803)

Written over 200 years ago in a letter to Dr. Benjamin Rush, the words of Thomas Jefferson still offer food for thought. Then, the issue was religious freedom. Today, the primary issue is the right to privacy. The right to privacy was not explicitly stated in the Constitution of the United States. However, many (including the Supreme Court) have argued that the right to privacy is an integral part of the constitution, as well as implicit in the thoughts and ideas of the Founding Fathers. In 1890, Samuel Warren and Louis Brandeis wrote an essay entitled "The Right to Privacy." At the time, the ease with which personal information, including photographs, could be disseminated to the public was beginning to make many citizens feel uneasy with respect to their own personal information. Warren and Brandeis argued that individuals should have control over their own personal information and that common law protects the right to privacy. Although the debate about whether, as citizens, we have a right to privacy has raged on for many decades since this famous essay, the decision in *Griswold v. Connecticut* (381 U.S. 479) in 1965 marked the beginning of constitutional protection for the right. This decision overturned the convictions of the director of Planned Parenthood and a doctor at Yale Medical School for dispersing contraceptive-related information, instruction, and medical advice to married persons. It has been used to protect the rights of many citizens including, most famously, the right to have an abortion in the case of *Roe v. Wade* (410 U.S. 113) in 1973. Although the applicability of this decision to specific activities has and will continue to be questioned, the "right to one's personality" discussed by Warren and Brandeis is an unmistakable part of the fabric of legal and political tradition in the United States of America.

The horrific events of September 11, 2001, have been an undeniable force affecting privacy. On this day, millions of people sat and watched in a state of disbelief as thousands of Americans lost their lives to the hate-inspired actions of others. How could this have happened? Why were we not protected? What should we do to make

sure this does not happen again? Questions, anger, and more questions filled the public dialog. Unfortunately, this was not the first time the security of American citizens had been threatened on American soil. It was also not the first time that personal rights came under attack. The Alien and Sedition Acts, the suspension of habeas corpus during the Civil War, the internment of Japanese-Americans during World War II, the McCarthy era, and the surveillance and harassment of antiwar protesters, including Dr. Martin Luther King Jr., during the Vietnam War all mark serious transgressions against the right of privacy by those in power during different periods of our nations history. During times of crisis and war, two things can be expected. First, the power of the president will be at its highest, and personal liberties and freedoms will be at their lowest. This follows the political theory of Thomas Hobbes, who reasoned that citizens must expect to give up some of their freedoms in return for protection and a civil society.

The USA Patriot Act was signed into law October 26, 2001, after passing in the House of Representatives by a vote of 357-66, with nine not voting, and in the Senate by a vote of 98-1, with one not voting. Coming on the heels of 9-11, this law was rushed to a vote and provided the executive branch with the power it felt it needed to fight terrorism and those responsible for one of the darkest days in our nation's history. It was also, unfortunately, one of the greatest assaults on personal privacy ever launched upon the citizens of our nation. This sentiment is echoed by the words of the one Senator, Russ Feingold, who voted against the measure.

There is no doubt that if we lived in a police state, it would be easier to catch terrorists. If we lived in a country that allowed the police to search your home at any time for any reason; if we lived in a country that allowed the government to open your mail, eavesdrop on your phone conversations, or intercept your email communications; if we lived in a country that allowed the government to hold people in jail indefinitely based on what they write or think, or based on mere suspicion that they are up to no good, then the government would no doubt discover and arrest more terrorists. But that probably would not be a country in which we would want to live. That would not be a country for which we could, in good conscience, ask our young people to fight and die. In short, that would not be America.

Despite assurances to the contrary, the fears expressed by opponents of the Patriot Act have manifested themselves time and again. The abuse of prisoners at Abu Ghraib prison signaled that the Bush administration was willing to violate basic human rights in order to secure information. That studies indicate that torture as a means to collect information is unreliable, at best, appears to have been lost on the Bush administration. The warrantless wiretapping of American citizens reveals a sense of imperial power that many scholars and lawmakers viewed as unconstitutional long before it was rebuked by federal judges. The classification of investigations that collect and warehouse data on American citizens as being terrorism-related when

there were no terrorism links present suggests a willingness to accumulate data on ordinary citizens. For citizens who believe that if they are doing nothing wrong then they have nothing to worry about, this should serve as a wake-up call. What is even more troubling is that when the investigations turn out to not be related to terrorism, the classification code used to mark the type of investigation is never changed to something that would indicate it is not terrorism-related. This indicates either a major problem with responsible management of personal information or a deliberate attempt to inflate antiterrorism statistics. Either is cause for concern. Finally, in March 2007, the abuse of power that is enabled by many of the provisions of the Patriot Act boiled to a head as an audit of the FBI use of National Security Letters (NSL) was made public.

The FBI issued about 8,500 NSLs in 2000, the last full year before the Patriot Act was passed. Four years later, the reported use of NSLs peaked at 56,000. Altogether, 143,000 NSL requests occurred from 2003-2005. NSL's are issued to organizations requesting that they turn over various record and data pertaining to individuals. NSL's require no judicial oversight. The original Patriot Act provision prohibited recipients from ever disclosing their receipt of an NSL to anyone. The Patriot Act expanded the use of NSL's by requiring that they only be relevant to an authorized investigation of international terrorism or foreign intelligence and that it not burden activities protected by the First Amendment. The lack of judicial oversight and the limits placed on free speech are troubling. The fact that the FBI misused this power several times, as found in a small audit of cases, is also troubling. These facts combined with the finding that "exigent letters," a letter that essentially circumvents the NSL process, were used over 700 times during the audit period, may have opened a policy window for change.

Many of the chapters in *Patriotic Information Systems* echo the sentiment of Senator Feingold in examining many of the current attacks on core democratic ideals, including the right to privacy. The first chapter in the book, entitled "Bush Administration Information Policy and Democratic Values," is written by G. David Garson and serves as an introduction to many of the issues presented in the course of the book. Discussions of the Total Information Awareness Act (TIA) and the USA Patriot Act are used to illustrate the concern over the survival of democratic values in what is increasingly a surveillance society. The chapter concludes with policy recommendations for fighting terrorism while protecting the freedoms of citizens.

The next five chapters comprise a section of the book that deals with the freedom of information and access. In his chapter "Less Safe: The Dismantling of Public Information Systems after September 11," Harry Hammitt analyzes how, in response to perceived security threats, government agencies have taken information down from Web sites, curtailed or restricted access to electronic sources of information, broadened the interpretation of FOIA exemptions, created or augmented new categories of restricted information, and prohibited public access for critical infrastructure information. These policy responses have been based both on the perceived security threat and an inhospitable attitude toward open government on

the part of the Bush administration.

Next, Charles Davis, writing on "The Expanding of Privacy Rationales under the Federal Freedom of Information Act: Stigmatization as Talisman" focuses on the "War on Terror" and the handling of detainee and other information sought under the Freedom of Information Act suits by reporters.

Using two studies performed by the Library Research Center concerning the impact of the terrorist attacks and the USA PATRIOT Act on librarians and the patrons, Lauren Teffeau, Megan Mustafoff, and Leigh Estabrook combine to write a chapter entitled "Access to Information and the Freedom to Access: The Intersection of Public Libraries and the USA Patriot Act." The study finds a regional effect and points to the need for further research. The last chapter in the section on freedom of information and access is written by Abby A. Goodrum. The chapter serves as a national examination of librarians' perceptions of law enforcement activity in academic and public libraries and points to a possible chilling effect on the use and access of information.

The next section of chapters focuses on security, technology, and democracy. Brian S. Krueger, writing in "Resisting Government Internet Surveillance by Participating in Politics Online and Offline," argues that the growing use of the Internet for political participation and the government's expanded electronic surveillance capacities make increasingly dubious the assumption regarding political participation that citizens operate within an unproblematic surveillance context. Interestingly, Krueger finds that those who oppose the current administration, and who perceive the government monitors their Internet behavior, participate in politics online at the highest rates.

Jeffrey Roy's chapter on "Security, Sovereignty, and Continental Interoperability: Canada's Elusive Balance," discusses how U.S. antiterrorism and homeland security measures have raised international issues with respect to the appropriate scope of governmental action. As North American governance faces new and rising pressures to adapt to a post 9-11 nexus of security, technology, and democracy, the culture of secrecy already prevalent within U.S. national security authorities is being extended to the continental level under the guise of interoperability. Strikingly, this is happening without any corresponding political effort to ensure openness and public accountability, both within and between countries.

Akhlaque Haque, writing on "Information Technology and Surveillance: Implications for Public Administration in a New World Order," develops the thesis that the essential resolution of the Patriot Act has been to destabilize the status-quo, especially as it relates to diversity, by introducing control values. He argues that in trying to control apparent instability by surveillance methods, we could do more harm in the other branches of government, undermining the role of democracy in the information age. Finally, David C. Wyld, in "The Little Chip That Could: The Public Sector and RFID," provides a detailed examination of the current uses of RFID technology in the public sector. Like many things, the purpose for the technology will go a long way toward determining the effectiveness of the technology.

The final chapter entitled "Out of Control? The Real ID Act of 2005," is written by Todd Loendorf, and serves as the conclusion to the book. The chapter discusses the rationales for and arguments against the establishment of a Nation ID card, with particular attention paid to the issues revolving around the collection and mining of data. It concludes by illuminating the fact that this is a shining example of our federal system of government because, as of this writing, many states are actively seeking to repeal or amend this law.

In summary, the chapters in *Patriotic Information Systems* raise serious policy questions about current information policy of the U.S. government. It is now apparent that database technology can be used for various ends, ranging from promotion of democracy to strengthening of nationalism to shoring up authoritarian regimes through misinformation. When this is put in the context of the need for information technology (IT) security, with its nonparticipatory enforcement ethos, its inherent bias against freedom of information, and its massive claims on IT budget resources, the more secure IT systems of the future may well be even less hospitable to the democratic visions which some theorists once anticipated would be among the most important contributions of information technology to society.

References

Feingold, R. (2001, October 12). Address given to the Associated Press Managing Editors Conference, Milwaukee Art Museum, Milwaukee, WI.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, 4*, 193-220.