Government secrecy:

An ethical dilemma

Mary Beth Romo

San José State University

Summer 2014

Abstract

This paper examines theoretical aspects of information ethics and their relationship to civil and human rights. Secret government programs are often justified on the grounds of national security. However, their status is at odds with laws that guarantee equal opportunities and equal protection to individuals. The 2008 documentary film *Secrecy*, directed by Harvard University professors Peter Galison and Robb Moss, forms a framework with which to study these issues. This paper examines secret government programs that violate the rights to privacy and intellectual freedom, while at the same time serve to empower select groups within the government. The effectiveness of secret government programs in terms of how well they serve to protect individuals, the United States, and the Executive Branch of the government, are compared with their infringement on civil rights.

Table of Contents

Introduction

Are secret government programs justified by their effectiveness in ensuring national security? The evolution of the information age has enabled the United States government to collect data that could be valuable to national security, but these practices raise questions about infringements on civil rights (Freeman & Peace, 2005; Mason, 1986). Secret government surveillance programs may be too vast in scope to be of use in foreign intelligence investigations. The secrecy that surrounds these programs prevents proper congressional oversight, allowing unwarranted surveillance of innocent citizens. Intellectual freedom, a global right and an integral element to a democratic society, is at odds with secret surveillance (Maret, 2014, pp. 248-249). The founding fathers of the United States of America understood intellectual freedom to be a basic human necessity (Garoogian, 1991, p. 221). Classification systems that operate under the veil of secrecy suppress the open and free exchange of information. Secret government programs that challenge civil rights do not make the country safer, and secret power structures within the government are strengthened.

Methodology

Theoretical approaches to describe the concept of information form a basis for an inquiry into the role of information in fundamental human rights. This paper explores the establishment of legislation and precedents leading to the systematization of secret government programs. The 2008 documentary film *Secrecy,* directed by Harvard University professors Peter Galison and Robb Moss, investigates secret programs carried out by the United States government in the interest of national security. This film

provides a framework with which to analyze ethical issues surrounding government secrecy.

Theoretical and legal groundwork

Information provides the means to knowledge, which in turn forms the basis for cultural expression and self-realization. The pursuit of goals, which is an essential aspect of human nature, depends on information seeking. Information is necessary for rights to intellectual freedom, equal opportunity, counsel, and education. In order to participate fully in society, a citizen must be able to access information (Freeman & Peace, 2005; Mason, 1986). Therefore, humans must have political and moral rights to ensure free and equal access to information. This line of reasoning indicates the reciprocal nature of rights and duties. In this case, the individual's right to information implies society's duty to provide access to that information (Alfino & Pierce, 1997, pp. 38-41).

Privacy is referred to by philosopher Sissela Bok as "the condition of being protected from unwanted access by others- either physical access, personal information, or attention" (Bok, 1982, p. 10). In order to perceive oneself as distinct from one's surroundings, it is critical to have private space. Individuals protect their privacy by guarding their personal space (Bok, 1982, p. 11). Privacy forms the basis for dignity and relationships with others. Privacy, then, can be regarded as essential to humanity and an ethical necessity. The moral right to privacy of an individual must be protected. The Supreme Court of the United States has ruled that the right to privacy, including personal information, is ensured by the First, Fourth, Fifth, Ninth, and Fourteenth Amendments. The Privacy Act of 1974, Public Law 93-579, 88 Stat. 1896, addresses concerns about government acquisition and storage of identifiable personal information. It protects the

confidentiality of individual records, and restricts the use and sharing of this information by federal agencies (Garoogian, 1991, pp. 221-222; Privacy Act of 1974).

Since intellectual freedom, free speech, and privacy are all protected by Amendments to the Constitution, any control of free speech is an infringement of these rights. Robert Hauptman argues that rather than relying on legislation and court rulings to proscribe free speech, punishment should be subsequent to any harm that results from free speech (Hauptman, 2002, p. 16). It is difficult to imagine, however, the effectiveness of a punishment following the damage done by a person who exercised his right to free speech by publicly announcing nuclear missile launch codes. An opposing claim is that there are exceptions to free speech, particularly when safety is threatened (Etzioni, 1997). In certain instances, free speech is deliberately suppressed in order to conceal sensitive information. Sociologist George Simmel in 1906 referred to secrecy as "...purposeful concealment, that aggressive defense, so to speak, against the other party, which we call secrecy in the most real sense" (Maret, 2008, p. 4). Government secrecy, then, is defensible in cases where secrets, if revealed, would threaten the safety of the country. The question is how to strike a balance between security and constitutional rights.

National security

The emergence of government secrecy programs during World War II was preceded by voluntary self-censorship of nuclear physicists. The reason for the formal creation of modern government secrecy systems was to protect scientific research surrounding the development of the atomic bomb, known as the Manhattan Project. To prevent the enemy from obtaining this information, it was classified as '"secret," and was accessible only to a limited amount of authorized government personnel. Research was

conducted at several sites throughout the country, but the bombs themselves were designed at Los Alamos National Laboratory. Thousands of workers who were employed with the project were kept ignorant about the purpose of their work, while only a few understood the full scope of the project. Lieutenant General Leslie R. Groves, who headed the Manhattan Project, explained that secrecy was necessary in order to keep the information from: 1. the Germans, 2. the Japanese, 3. the Russians, 4. all other countries, and 5. other Executive agencies and the Congress who might interfere in the program. In other words, the purpose of the secrecy was to retain control and power (Galison & Moss, 2008).

United States v. Reynolds established a precedent of the State Secrets Privilege in cases where national security was at stake. The widows of three civilians who were killed in the 1948 crash of an Air Force B-29 Superfortress bomber sought damages in federal court. The Air Force refused to release details about the case, claiming that doing so would compromise a "Top Secret" mission. The case was the first recognition of the State Secrets Privilege. The Supreme Court did not review the documents that supposedly contained Top Secret information. Ironically, the declassified accident report revealed that the plane crash was due to mechanical problems and negligence on the part of the Air Force. Though secret equipment was onboard, the crash had nothing to do with a secret mission. This precedent, set on a lie, has been cited hundreds of times since (Galison & Moss, 2008).

Threat of terrorism

Subsequent to the establishment of the State Secrets Privilege, Executive Orders and legislation systematized secrecy (Maret, 2014, p. 256). Following the terrorist attacks

of 9/11, the USA PATRIOT Act, Public Law 107 –56, 115 Stat. 272 (USA PATRIOT Act), was quickly adopted in order to enable law enforcement and intelligence agencies to more efficiently discover terrorist plots and avert further attacks. Section 215 allows the Federal Intelligence Surveillance Court (FISC) to issue secret surveillance orders on foreign individuals and U.S. citizens suspected of being foreign agents. Though checks and balances are provided by the Act to prevent abuse by law enforcement, questions have been raised as to whether or not the law is at odds with constitutional rights. The American Library Association (ALA) questioned the prohibition by the FISC of any communications once a surveillance order was served. The secrecy surrounding these actions is in opposition to the rights provided by the First and Fourth Amendments (Coolidge, 2005).

Furthermore, FISC requirements for obtaining a surveillance order do not apply to presidential authorization for the surveillance of electronic communications by the National Security Agency (NSA) without a court order, for the purpose of gathering foreign intelligence information. This authorization was originally granted by the Protect America Act of 2007, Public Law 110-55, 121 Stat. 552 (Protect America Act of 2007). The Senate subsequently passed a bill that amended FISC search warrant requirements (FISA Amendments Act of 2008).

The modern world landscape presents new terrorist threats for which outdated Cold War strategies are ineffective. In order to contend with such threats, the CIA asserts its need to fight a "clandestine war using methods counter to values of the United States" (Galison & Moss, 2008). These methods include the use of torture on prisoners, as epitomized by the practices at Abu Ghraib. Initial reports of these criminal activities were

classified secret. The reoccurrence of these and similar acts that may be considered war crimes throughout the course of history underline the emergence of evil human tendencies in the presence of secrecy and unchecked power. Paradoxically, the employment of inhumane methods in the effort to spread democracy is contrary to the very foundations of the democratic system.

In November 2001 President Bush issued a Military Order establishing secret military tribunals. Disclosures about the experiences of foreign terrorist suspects detained by the United States provide evidence that concerns about the lack of accountability in secret proceedings are well founded. Salim Hamdan was arrested in November 2001 at the border of Afghanistan and Pakistan, charged with terrorism, and sent to Guantanamo Bay after admitting to having been Osama Bin Laden's driver. He was charged by a secret military tribunal and denied the rights of habeus corpus under Bush's Military Order. Secret military tribunals in which the president had unlimited powers were conducted with deliberate disregard for the basic foundations of the judicial system of the United States (Galison & Moss, 2008).

> Neal Katyal, attorney for the plaintiff in the case of Hamdan v. Rumsfeld states: If the president is taking secret actions that violate laws passed by Congress, treaties ratified by the Senate, and doing it in the name of Executive Power, one might think that's permitted on September 15, 2001, but years later it is a fundamentally corrosive threat to democracy (Galison & Moss, 2008).

In 2003 Khaled el-Masri, an innocent German citizen, was wrongfully arrested by the Central Intelligence Agency (CIA), and tortured in a secret prison. The American

Civil Liberties Union (ACLU) brought charges against the CIA, who requested the lawsuit to be dismissed based on the privilege of State Secrets. They claimed that litigation would reveal information that could damage national security. The CIA eventually released El-Masri, admitting that his arrest was a mistake. El-Masri's case is an example of the abuses that occur under the veil of secret government programs (Galison & Moss, 2008).

The government uses the States Secret Privilege to declare itself immune to the judicial process. Immediately after a case is filed, the claim for it to be dismissed in the interest of national security prevents any further scrutiny of the ostensibly secret evidence (Galison & Moss, 2008). This lack of oversight may result in the abuse of power.

Electronic surveillance

"Open source intelligence" refers to the collection of information that is already freely available in the public domain, from sources such as newspapers, radio, television, and the Internet, and using it for a specific intelligence purpose. The United States government has been involved in such activities since World War II, but the collection of open source information has taken on a more urgent role post-9/11. The secret and institutionalized practice of gathering and analyzing open source information is at variance with safeguards provided by the Privacy Act of 1974. However, the "ambiguity of the meaning of 'open source' obscures public understanding of the ethical dimensions of this phenomenon and its associated practices" (Bean, 2011, p. 386).

Edward Snowden, former contractor for the NSA, has revealed that secret surveillance is not limited to foreign terrorist suspects, but also includes innocent U.S. citizens. Secret global surveillance of all electronic communications by the NSA not only

violates privacy, but also raises questions as to the effectiveness of such a vast program (Maret, 2014, pp. 284-285; Munk debates, 2014). It has been argued that "the U.S. intelligence community's failure to adequately collect and analyze open source information is potentially wasteful, inefficient, and dangerous" (Bean, 2011, p. 388).

Secret electronic surveillance, justified by the government on the grounds of national security, compromises the security of the Internet. If Internet users lose trust in online security because they are suspicious that the government is spying on their activities, the efficiency, freedom, and meaningfulness of the World Wide Web are diminished. Government secrecy, in this instance, reduces security (Munk debates, 2014).

Information is power

Perceptions are grounded in thoughts, which in turn are based on processed information. In his book on *Ethics of information management*, Richard Mason describes information as the symbolic means by which one mind influences another mind (Mason, 1995, p. 35). Decision-making and self-realization are dependent upon access to information. Mason argues that "the unique characteristics of information... facilitate its use in developing impressions and making decisions. This relates directly to the central role that information plays in decision making" (Mason, 1995, p. 47). For this reason, information has become the world's most valuable commodity.

Mason argues that the giving, orchestrating, and taking of the unique resource of information are a basic source of power (Mason, 1995, pp. 40-41). If one can limit, repress, and distort information under a veil of secrecy, it becomes possible to shape perceptions and control ideas. Controlling the flow of information, then, is a means to empowerment (Hauptman, 2002, p. 16).

Censorship

New ideas, which are also the result of perceptions, can threaten established power structures. Unacceptable ideas are controlled, repressed, or eliminated through censorship (Jensen, 2004, p. 28). Censorship takes many forms, all of which are inextricably linked to secrecy. In "Nature and Function of Secrecy and Propaganda" from his 1972 *The Pathology of Politics*, political scientist Carl J. Friedrich connects secrecy with a "tampering of communications," and associates the practice with repressive governments (Maret, 2008, p. 5). Government agencies that are granted the use of the State Secrets Privilege are thus granted the power to control information, which in turn generates more power (Maret, 2014, pp. 256-257).

Provisions of the USA PATRIOT Act required the withdrawal of information that was previously accessible by the public. The cost of keeping billions of pages of historical documents secret is estimated to be $7.5 billion per year (Galison & Moss, 2008). Secrecy programs are inherently opposed to the right to free access to information. The American Library Association (ALA) defends the public's need for access to information and the free and open exchange of knowledge in its *Resolution on Disinformation, Media Manipulation & the Destruction of Public Information*. The ALA states its objection to government censorship, including the omission, destruction, distortion, and editing of information for the purpose of enhancing power (American Library Association, 2005).

In 2003 the United States launched the Gulf War against Iraq based on the assumption that the country, under President Saddam Hussein, was producing and storing weapons of mass destruction (WMD). While U.S. inspectors discovered no evidence of

WMD, senior officials in Washington held press briefings at which they stated their "high confidence" that WMD would be found. Though the official account of the findings was a distorted version of reality, a truer version was reported by journalists who were present at the inspections (Galison & Moss, 2008).

Research pertaining to climate change conducted by federal scientists during the Bush-Cheney Administration produced evidence of substantial threats to the environment. However, the Administration and its appointees to key positions controlled the flow of information to the public, the media, and Congress. Reports that were counter to the Administration's interests were edited, withheld, and distorted. Scientists were unable to get approval for press releases and were forbidden to speak to the media. Government websites were inexplicably shut down. Agency scientists' reports to Congress that outlined negative consequences of greenhouse emissions were altered in such a way that the meaning was changed. The only research that was communicated was that which supported the policies of the Administration. Censorship of scientific findings prevented implementation of policies that would reduce harmful emissions of greenhouse gases, thereby imposing dangers to the entire nation, the environment, and the future of the planet (Piltz, 2001). Propaganda that protects elite power structures goes against the ideals of a democratic state. Government secrecy, in this case, did not provide security for the country.

Government secrecy creates a tension between the power over information and the public right to know (Maret, 2008, p. 13). Secret government programs that control the flow of information hinder free and equal access, thus reducing the security of individuals in their rights to live freely and pursue happiness in a democratic society.

Consequently, governments secrecy does *not* ensure that individuals are made more secure in their rights and does *not* render them safer from harm.

No checks and balances

Government secrecy programs undermine the very principles on which the United States is based. Intellectual freedom, a crucial aspect of democracy, requires freedom from unwarranted surveillance (Maret, 2014, p. 248). In direct violation of this right are secret government surveillance programs that collect, mine, store, and analyze electronic communications, offering no explanation as to the reason for the secrecy. These practices are incompatible with the Privacy Act of 1974. The employment of private contractors to aid in this project raises further questions about conflicting interests and breaches of privacy rights (Bean, 2011, p. 391).

Though the purpose of NSA surveillance of electronic communications is to stop terrorism, they have failed to produce any examples of actual threats that have been averted as a result of secret surveillance (Munk debates, 2014). On the other hand, excessive secrecy and *overclassification* was partly responsible for preventing federal terrorist investigators from thwarting the 9/11 attacks. The Commission investigating the attacks found that secrecy hampered the operation of national security efforts. Secret information was compartmentalized and restricted, inhibiting investigators from sharing and assembling information that surely would have led to a greater understanding of the unfolding events. Counter-terrorism would be best served by an informed and alert public. The capture of the Unabomber after the publication of his manifesto demonstrates a case where publicity, rather than secrecy, led to greater safety (Galison & Moss, 2008).

Secrecy allows for no checks and balances to restrain power. Secret bureaucratic power structures within the government operate without proper oversight. As a result, secrecy empowers and protects select elite groups, without the knowledge or consent of the public or the other branches of government. Any monopoly on information by one branch of the government curtails the ability of the other two branches to make good decisions. Placing one branch at an advantage defeats the purpose of controls provided by the separation of powers (Galison & Moss, 2008; Maret, 2014).

In 1955, a Special Government Information Subcommittee convened by Congressman John Moss "led to greater understanding of security classification in the Executive Branch, the fundamental ways secrecy impairs relations of Congress with the Executive Branch as well as damages citizen confidence in government through lack of knowledge on policies and policy making" (Maret, 2008, p. 10). The 1997 Commission on Protecting and Reducing Government Secrecy (the Moynihan Commission) was a statutory commission to examine government secrecy. It established secrecy as a form of government regulation. Many of the Commission's recommendations were not implemented (Maret, 2008, p. 10).

Information ethics in the age of technology

In order to preserve the freedoms granted in a democracy, such as free speech, intellectual freedom, and the right to privacy, government programs must operate ethically and respect the intentions of the Constitution. As Kent Cooper of the Associated Press pointed out in January 1945, "there cannot be political freedom in one country or the world, without respect for 'the right to know'" (Maret, 2008, p. 8). The adherence to the fundamentals of a free democracy is of particular importance during times of unrest

and fear, when principles and ethics have a tendency to be overlooked. In the new political landscape, where the fear of terrorism has led to the abandonment of democratic principles, it is crucial to uphold the foundations on which the United States was built.

As the future moves toward an environment in which humans become increasingly dependent on digital information and technology, ownership and control of information take on an unprecedented value. While public understanding of government data collection programs is questionable, and legislation struggles to respond, personal information continues to be gathered and stored. An ethical approach to the collection, storage, and use of information must be established (Floridi, 2010). Since an ethical perspective on information threatens the control-oriented field of intelligence (Bean, 2011, p. 388), legislation and oversight are critical. A free and democratic society requires that the government handles information with transparency, and that these practices are subjected to judicial review (Freeman & Peace, 2005; Mason, 1986; Wilkinson & Gerolami, 2009, p. 329).

When asked whether the United States is safer now than it was 10 years ago, Lt. Gen. Michael Flynn, head of the Defense Intelligence Agency, states, "My quick answer is we're not." Flynn was interviewed on July 26, 2014 at the Aspen Security Forum, where top counterterrorism officials addressed questions about national and homeland security. Denying Obama administration claims that core Al Qaeda is on the run, he counters that the ideology behind it is "exponentially growing." Flynn says, "We have a whole gang of new actors out there that are far more extreme than Al Qaeda" (Aspen Security Forum, 2014).

Conclusion

Government secrecy programs that exist for the purpose of national security have not made the United States of America safer. Secret control of the flow information obstructs intellectual freedom. Though technological advancements have increased the ability of the government to carry on global electronic surveillance programs, questions remain as to the purpose and effectiveness of these programs, as well as their ability to withstand the scrutiny of the Constitution of the United States. Without proper oversight by the legislative and judicial branches of the government, as well as an informed public, it is impossible to answer these questions.

References

Alfino, M., & Pierce, L. (1997). A philosophical understanding of the moral value of information. *Information ethics for librarians* (pp. 23-56). Jefferson, NC: McFarland & Company.

American Library Association. (2005). *Resolution on disinformation, media manipulation, and destruction of public information*. Retrieved, 2014, from http://www.ala.org/aboutala/sites/ala.org.aboutala/files/content/governance/policymanual/updatedpolicymanual/ocrpdfofprm/52-8disinformation.pdf

Aspen Security Forum. (2014). Retrieved August 11, 2014, from http://aspensecurityforum.org/media/live-video/

Bean, H. (2011). Is open source intelligence an ethical issue? In S. Maret (Ed.), *Government Secrecy, Research in social problems and public policy,* volume 19 (pp. 385-402). Emerald Group Publishing Limited. doi:10.1108/S0196-1152(2011)0000019024

Bok, S. (1982). Approaches to Secrecy. *Secrets: on the ethics of concealment and revelation* (pp. 3-14). New York: Pantheon Books.

Coolidge, K. K. (2005). "Baseless hysteria": The controversy between the Department of Justice and the American Library Association over the USA PATRIOT Act. *Law Library Journal, 97*(1), 7-29.

Etzioni, A. (1997). The First Amendment is not an absolute even on the internet. *Journal of Information Ethics, 6*, 64-66.

FISA Amendments Act of 2008, Pub. L. No. 110-261. 122 Stat. 2463. (2008). Retrieved from

http://www.gpo.gov/fdsys/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf

Floridi, L. (2010). Ethics after the information revolution. In L. Floridi (Ed.), *The Cambridge handbook of information and computer ethics* (pp. 3-19). Cambridge; New York: Cambridge University Press.

Freeman, L. A., & Peace, A. G. (2005). Revisiting Mason: The last 18 years and onward. *Information ethics: Privacy and intellectual property* (pp. 1-18). London: Information Science Publishing.

Galison, P., & Moss, R. (Directors). (2008). *Secrecy* [Documentary]. United States: Redacted Pictures.

Garoogian, R. (1991). Librarian/Patron confidentiality: An ethical challenge. *Library Trends, 40*(2), 216-233.

Hauptman, R. (2002). Intellectual freedom and the control of ideas. *Ethics and librarianship* (pp. 16-29). Jefferson, NC: McFarland.

Hauptman, R. (2002). Why ethics matters. *Ethics and librarianship* (pp. 132-140). Jefferson, NC: McFarland.

Jensen, R. (2004). The myth of the neutral professional. *Progressive Librarian, 24*, 28-34. Retrieved from http://progressivelibrariansguild.org

Levine, M. (2014, July 27). US Less Safe Than Several Years Ago, Top Intelligence Official Says. *ABC News.* Retrieved from http://abcnews.go.com/

Maret, S. (2014). Intellectual freedom and U.S. government secrecy. In M. Alfino, & L. Koltutsky (Eds.), *The Library Juice Press handbook of intellectual freedom: Concepts, cases, and theories* (pp. 247-281). Sacramento, CA: Library Juice Press.

Maret, S. & Goldman, J. (2008). Introduction. *Government Secrecy: Classic and Contemporary Readings* (pp. 1-20). Westport, CT: Libraries Unlimited.

Mason, R. O. (1995). Information: Its Special Nature. *Ethics of information management* (pp.35-48). Thousand Oaks, CA: SAGE Publications, Inc.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), 5-12.

Mulrine, A. (2014, July 28). US is no safer after 13 years of war, a top Pentagon official says. *Christian Science Monitor.* Retrieved from http://www.csmonitor.com

Piltz, R. (2011). Secrecy, complicity, and resistance: Political control of climate science communication under the Bush–Cheney Administration. In S. Maret (Ed.), *Government secrecy, Research in Social Problems and Public Policy*, volume 19, (pp. 219-246). Emerald Group Publishing Limited.

Privacy Act of 1974, Pub. L. No. 93-579. 88 Stat. 1896. (1974). Retrieved from http://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf

Protect America Act of 2007, Pub. L. No. 110-55. 121 Stat. 552. (2007). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm

State surveillance, *Munk debates*. (2014). Retrieved July 3, 2014, from http://www.munkdebates.com/debates/state-surveillance

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107 –56. 115 Stat. 272. (2001). Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS107hr3162enr/pdf/BILLS-107hr3162enr.pdf

Wilkinson, M. A., & Gerolami, N. (2009). The author as agent of information policy: The relationship between economic and moral rights in copyright. *Government Information Quarterly, 26*(2). doi:10.1016/j.giq.2008.12.002