Chapter 53
Reconciling the Needs for National Security and Citizen Privacy in an Age of Surveillance

Kenneth L. Hacker
New Mexico State University, USA

Bridget Acquah-Baidoo
New Mexico State University, USA

Anthony Epperson
New Mexico State University, USA

ABSTRACT

This chapter explores important ethics issues regarding government surveillance on citizens. Two views are discussed regarding debates about ethics and possible model development for reconciling tensions between freedom and security. Key issues for debate are presented and these include the need to define and deliberate the meanings of privacy, abuse, proportionality, secrecy, etc. Certain propositions for debate are also offered. These are: a. It is unethical to monitor citizens who are not under any demonstrable reason of suspicion without their knowledge or permission; b. It is unethical for citizens to block necessary national security surveillance when such surveillance is proven to be needed to stop acts of crime or terrorism; c. Governments should not conceal the facts about how much they monitor citizens for national security and in what typical conditions they do so; and d. Citizens should not accuse governments who use surveillance to track criminals and terrorists as being fascists or trying to establish dictatorships.

Those who surrender true liberty to a false security defend nothing worth preserving, while those who abandon real security to an illusory liberty protect nothing worth safeguarding. – Ronald Collins

We reject as false the choice between our safety and our ideals. – President Barack Obama

DOI: 10.4018/978-1-5225-0983-7.ch053

INTRODUCTION

It is commonly asserted that citizens in a democratic system must not only be informed about issues and free to express their views about those issues, but also free from unnecessary government intrusions on their freedoms and privacy. However, some political scientists like Flanigan and Zingale (2002) observe that Americans may have stronger commitments to democratic goals than to specific practices supporting those goals. A general commitment to freedom from strong government intrusion has been evident in the United States since at least the 18th century and as a matter of historical precedent. However, other precedents have made present debates about liberties and privacy versus government surveillance more complex than the debates of the past. One precedent involves the rapid proliferation of various technologies of networking communication that make personal privacy something that individuals freely forfeit in exchange for apps, online purchases, website access, and other online privileges. Another precedent involves the rapid ease in which users can survey other users and governments (and corporations) can track, locate, and data mine online behaviors and users. Concurrently, the increased prevalence of security threats in hidden networks and asymmetric conflict have made intelligence efforts more keen on surveillance that has finer granularity of collected data and wider nets for data gathering. This goal of more focused and granular analysis is the result of government conclusions that threats to national security may be increasing at a faster rate than abilities to detect them are accelerating. There appears to be a continuing and unresolved conflict between the needs for privacy and the needs for national security.

There are two sectors of government that collect personal data on citizens and which have interests in increasing their abilities to do so in order to increase or protect national security: the intelligence community and law enforcement agencies. Intelligence agencies know that intelligence depends on data and the more data that can be gathered surreptitiously, the easier their tasks of analysis and detection. Law enforcement agencies seek to prevent crimes that are likely or possible of occurring and to use surveillance to track the behaviors of suspects likely to commit criminal acts. The key goals of the intelligence community (IC) and the law enforcement community (LEC) are to make predictions about likely criminal or terrorist activities and to intervene once analysis detects a dangerous plan that is likely to be carried out. For both communities, intelligence depends on data collection. IC and LEC professionals argue that they collect only data that is necessary. However, their critics say they collect more than what they need and move across the boundaries of what is ethical and appropriate in a democratic society.

The government makes its case for increasing surveillance and uses of surveillance technologies in many venues including court cases, statements by political leaders, and discourse produced by intelligence and law enforcement professionals. For example, it is common for the IC to note that the NSA does massive amounts of data mining in order to look for signs in the data that may indicate possible terrorist activity or planning. NSA researchers believe that data mining and aggregation allows them to build profiles that indicate certain dangers. Data include phone call records, financial transactions, and travel information (Lee, 2013). However, some data scientists doubt the ability of the National Security Agency (NSA) to develop the profiles it claims it can make (Lee, 2013). If they are correct, some of the thunder from the government defense of its privacy intrusions may be diminished.

Concerned citizens, journalists, scholars, and political activists make a case which says that government is overstepping its legitimate authority by its continuing intrusions on personal privacy. It is noted that there are many historical examples in the United States of political power being abused by the use of government surveillance. For example, the FBI bugged about 14 hotel rooms where Martin Luther King stayed and then sent him a letter threatening to release some of the recordings which might discredit Dr.