INFORMATION SCIENCE PUBLISHING ITB10544
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

Chapter X

Counterterrorism and Privacy:

The Changing Landscape of Surveillance and Civil Liberties

Michael Freeman
Dartmouth College, USA

Abstract

*This chapter addresses how new surveillance technologies and programs aimed at fighting terrorism affect privacy. Some of the new programs and technologies considered include the USA PATRIOT Act (**U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism), biometrics, national ID cards, video surveillance, and the Total Information Awareness program. This chapter first evaluates the pre-9/11 status quo in terms of what techniques were used, and then examines how the new technologies and programs that have recently been implemented affect privacy constitutionally, legally, and normatively. This chapter argues that many of the recent changes do not, in fact, undermine privacy at a constitutional or legal level, but do run counter to what Americans want and expect in terms of privacy.*

Introduction

New surveillance technologies and government programs are being rapidly developed and implemented to fight terrorism, but pose serious challenges to civil liberties and privacy rights. For instance, the PATRIOT Act, the Total Information Awareness program, and national ID cards have all been hotly debated as everyone from libertarians to librarians have worried over how these new programs redefine how the government conducts surveillance of suspected terrorists. At the heart of many of these programs are new technologies such as advanced data-mining software, facial recognition devices, retinal scanners, and other advances in biometrics.

The goal of this chapter is to address how these new technologies and programs can be understood in relation to privacy concerns. To do so, we first need to look at the right of privacy from several angles, specifically, how it is conceived constitutionally, legally, and normatively (by looking at public opinion). Afterwards, various surveillance methods will be divided into three broad types: communications surveillance, information surveillance, and identity surveillance. Communications surveillance looks at what people say or write over e-mail or the phone; the PATRIOT Act is the major source of change in how this information is obtained. Information surveillance looks at the records people have at various places, like banks, hospitals, libraries, etc. New database mining software, the Total Information Awareness project, and provisions in the PATRIOT Act have changed how we think about this type of surveillance. Identity surveillance tracks who you are, possibly with biometric identifiers, or where you are, with video cameras and face recognition technology. For each of these surveillance types, this chapter will evaluate the pre-9/11 status quo in terms of what techniques were used and how they impacted privacy concerns and then examine how the new technologies and programs that have recently been implemented change the pre-9/11 status quo.

Assessing Technology's Impact on Privacy

With the passage of the PATRIOT Act and technological advances in surveillance and biometrics, the future of privacy has been hotly debated. On one side, the ACLU claims, "the surveillance monster is getting bigger and stronger by