Chapter 10
Culture Clashes:
Freedom, Privacy, and Government Surveillance Issues Arising in Relation to National Security and Internet Use

Pauline C. Reich
Waseda University, Japan

ABSTRACT

This chapter reviews fundamental U.S. constitutional law in relation to privacy; the various United States federal privacy laws in relation to government surveillance of online communications by private citizens; cases related to these issues, recent amendments and proposed amendments to U.S. law; comparisons to law in other countries. It concludes that this particular area of law, at least in the United States, United Kingdom, India, Australia, and Canada, which continues to be hotly debated, has no resolution in sight, and the difficult problem of balancing national security and privacy while maintaining constitutional protections in democracies is still a problem in search of a solution.

1. INTRODUCTION

Professor Jack Balkin of Yale Law School may have hit the nail on the head when he described the advent of the "Surveillance Society" in the United States in a law journal article published a few years ago (Balkin, 2008). With our growing use of the Internet and other information and communication technologies, there has been the parallel use by the law enforcement and national security communities of surveillance of online communications, digital forensics, etc. Balkin says it is inevitable – however the extent to which the average citizen is monitored raises legal and policy issues related to freedom of the Internet, privacy and civil liberties.

DOI: 10.4018/978-1-61520-831-9.ch010

There are various sectors battling this out in United States courts and Congress: the so-called "privacy lobby"(derided by some experts from outside the military and intelligence communities) (Baker, 2010), who have been litigating issues concerning government-ordered telecommunication company surveillance during the Bush administration and who continue to litigate (Kravets, 2011, *Jewel v. NSA*, 2011, *Jewel v. NSA Full Complaint*, 2011); the Internet freedom philosophers and theorists who worry that the Internet will morph from the Wild West mode to one in which communications and use are limited by regulations, governments, etc. (Bradshaw, 2011, Berners-Lee, 2010). Technologists looking at the redesign of the Internet so that it is no longer open to all, but perhaps carved up into a variety of separate networks with varying kinds of access, or made more secure, particularly for government and business purposes (Shanker, 2010).

This chapter will examine the evolution of the law surrounding surveillance by governments in democracies of Internet use and the resultant litigation; technological measures put into place for protection of national security, etc.; policy and law with respect to Internet surveillance by governments, law enforcement, and currently private sector companies and Internet Service Providers (ISPs), etc.

2. PRE-INTERNET AND CURRENT LEGISLATION AND CALLS FOR JUDICIAL REVIEW AND AMENDMENT

2.1. The Fourth Amendment of the U.S. Constitution: What Does It Mean These Days?

A Congressional Research Service report published in 2006 reviews the Fourth Amendment to the Constitution, which provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

While the right against unreasonable searches and seizures was originally applied only to tangible things, Supreme Court jurisprudence eventually expanded the contours of the Fourth Amendment to cover intangible items such as conversations. As communications technology has advanced, the technology for intrusion into private conversations has kept pace, as have government efforts to exploit such technology for law enforcement and intelligence purposes. At the same time, the Court has expanded its interpretation of the scope of the Fourth Amendment with respect to such techniques, and Congress has legislated both to protect privacy and to enable the government to pursue its legitimate interests in enforcing the law and gathering foreign intelligence information. Yet the precise boundaries of what the Constitution allows, as well as what it requires, are not fully demarcated, and the relevant statutes are not entirely free from ambiguity (Bazan & Elsea, 2006).

Since the terrorist attacks of 9/11/01 (and even before), there has been ongoing legislation and litigation in the United States concerning the application of the Fourth Amendment to wiretapping and other forms of electronic surveillance by government agencies and the police of (1) suspected criminals and terrorists; (2) the average citizen.

The story is much too long, complex and detailed to recount in its entirety here (Harris, 2010). The Congressional Research Service (CRS) and the Government Accountability Office (GAO) have written explanatory reports concerning the legislative developments, if not the litigation, which may be useful to the reader. An excerpt of one of these reports appears in Appendix I of