Chapter XII

The Public Policy Environment of the Privacy–Security Conundrum/Complement

John W. Bagby
Pennsylvania State University, USA

ABSTRACT

Public policy constraints impact deployment of most technology underlying the convergence of digital technologies in telecommunications, e-commerce, and e-government. Networked computers increase the vulnerability of confidential data, transaction processing infrastructure and national security. Compliance regulation imposes complex constraints on data management by government, the private-sector and their personnel. Privacy and security are a balance between individual interests in secrecy/solitude and society’s interests in security, order, and efficiency. This chapter explores the key political, legal, and regulatory methods for resolving conflicts between privacy rights and security methods to encourage convergence success. The “Privacy-Security Conundrum” is framed, then set against the more cross-dependant relationships of a “Privacy-Security Complement.” Security law illustrates that the conundrum-complement dilemma serves to define convergence as constrained and induced by the legal and policy perspectives or privacy, intellectual property, technology transfer, electronic records management, torts, criminal law, fiduciary and contractual duties and professional ethics regulating privacy and security.

INTRODUCTION

Public policy constraints are likely to impact the deployment and continuing operation of nearly any technology, method or process designed to support counter-terrorism. Policy drives the traditional institutional efforts to maintain security. These have been focused on criminal enforcement and regulatory risks based on commonly-held understandings of burglary, theft, conversion and other protections of physical property. However, such a focus largely on physical security protections for tangible property is inconsistent with the proliferation of networked computers and their impact on the economy and key infrastructures (Exec. Order No. 13,231, 2001). The latter has vastly...
increased the vulnerability of confidential-private data, transaction processing and critical national security systems. At the heart of these challenges lies regulatory compliance with security and privacy laws. Such responsibility now falls much more clearly on all levels of government (local, state/provincial, national/federal and regional/international) as well as on the private-sector and on individuals. These complex new duties constrain organizations in the data management industry as well as suppliers and users of data and all participants in the information supply chain, a useful conceptual framework discussed in this chapter. Such participants include consultants, software suppliers, applications service providers, out-sources of maintenance and communications intermediaries.

Privacy and security will likely remain in a balance between individual interests in secrecy/solitude and society’s interests in security, order and efficiency. Privacy is a fragmented, assortment of rights found in international law, constitutions, federal statutes and regulations, state statutes and regulations, common law precedents and private contracts. Many of these sources of law can simultaneously exhibit conflicts, complements and direct or indirect referencing. This Chapter frames the privacy rights debate in two ways: as a conundrum or tradeoff with security and alternatively as a complement between these two concepts. The conundrum/complement model provides insight for policy makers who constrain and enable the design of information and communications technologies (ICT). These policies inform the identification and resolution of policy concerns throughout the design and implementation process. These are policy analysis tools that can advance technology implementation by attenuating public surprise of privacy intrusions and thereby improve the opportunities for technological convergence.

This article explores the converging fields of privacy rights and security in light of legal duties and public policy under American and International laws. Several key factors are examined: public policies underlying regulation of privacy and security, insights into how society accommodates transition of existing laws to the unique vulnerabilities of government and the information economy, management of employment and independent contractor relations for privacy and security and the processes used at many government agencies to regulate privacy and security. There is an analysis of recurring privacy and security experience in some particular industry “sectors.”

**CONCEPTUAL PRIVACY AND PUBLIC POLICY**

Privacy is understood more fully if seen through fundamental and enduring historical and social expectations. Privacy can be viewed from its Biblical origins. As early as the Garden of Eden, privacy concepts of shame and modesty signaled the inevitable imperfection of human decision-making and the will to avoid embarrassment. Abundant privacy lowers the human risk of public contempt or retribution. Similarly, modesty, shyness and prudent appearance discourage societal predators. Privacy is an enduring, nearly universal, but elusive aspiration:

> Who could deny that privacy is a jewel? It has always been the mark of privilege. ... Out of the cave, the tribal tepee, the pueblo, the community fortress, man emerged to build himself a house of his own with a shelter in it for himself and his diversions. Every age has seen it so. The poor might have to huddle together ... [b]ut in each civilization, as it advanced, those who could afford it chose the luxury of a withdrawing-place. (McGinley, 1959)

Early American privacy rights protected citizens from intrusions by government, such as those suffered by early American colonists both as they