Chapter 7.4
Balancing the Public Policy Drivers in the Tension between Privacy and Security

John W. Bagby
The Pennsylvania State University, USA

ABSTRACT

The public expects that technologies used in electronic commerce and government will enhance security while preserving privacy. These expectations are focused through public policy influences, implemented by law, regulation, and standards emanating from states (provincial governments), federal agencies (central governments) and international law. They are influenced through market pressures set in contracts. This chapter posits that personally identifiable information (PII) is a form of property that flows along an "information supply chain" from collection, through archival and analysis and ultimately to its use in decision-making. The conceptual framework for balancing privacy and security developed here provides a foundation to develop and implement public policies that safeguard individual rights, the economy, critical infrastructures and national security. The illusive resolution of the practical antithesis between privacy and security is explored by developing some tradeoff relationships using exemplars from various fields that identify this quandary while recognizing how privacy and security sometimes harmonize.

INTRODUCTION

Public policy drives private enterprise and public institutional efforts to maintain security. A traditional focus on criminal enforcement and regulatory risks in the protection of physical property fails to adequately protect networked computers and the related impact on the national economy and critical infrastructures. Security failures make confidential-private data more vulnerable. These include vulnerabilities in the electronic transaction processing systems underlying electronic commerce and the systems supporting digital gov-

DOI: 10.4018/978-1-61350-323-2.ch7.4

ernment. National security is imperiled with any substantial weakening of the national economy. Fundamental to information assurance (IA) is regulatory compliance with both security and privacy law, responsibilities that are dispersed among (1) individuals, (2) government at all levels: local, state/provincial, national/federal, regional/ international, (3) private-sector entities generally and (4) specifically, private sector organizations in the burgeoning data management industry (e.g., suppliers and users of data, service providers to the "information supply chain"). Public policy must continually draw a balance between individual interests in secrecy or solitude and society's interests in security, order and efficiency. Privacy law in the United States is a fragmented, assortment of rights from various sources: constitutions, federal statutes and regulations, state statutes and regulations, standards, common law precedents and private contracts. This chapter frames the debate over privacy rights and security imperatives, first as a tradeoff, largely in the realms of national security and crimes, but then finds important points of complementarity between individuals' security and their privacy. Analysis using this model reveals insights for public policy makers that contribute to the implementation of technology by attenuating public surprise of privacy intrusions and enabling public support for reasonable security measures.

Confronting the professionals in the information technology (IT) industry who are most intimately engaged in IA, cyber-security and the facilitation of privacy protection, there is an often daunting complexity in public policy imperatives, because they are derived from law, standards, contracts, litigation and regulation and because the sources of these pressures are so varied. This uncertainty is particularly complicated for the control of personally identifiable information (PII) data security risks. A confluence of pressures now focuses on how vulnerabilities of tangible and intangible assets impact the reliability of information systems underlying transaction records. Internal control systems are the key mechanisms for the maintenance of security over information assets exerted through their influence over decision-making and operations monitoring in private-sector institutions, but with close analogs for public-sector institutions (Sarbanes-Oxley Act, 2002).

This chapter contends that to clarify IA threat reduction duties, IT professionals must more clearly understand public policy imperatives for internal control that emanate from evolving standards of professional practice and ethics, financial reporting standards, corporate governance, privacy law, trade secret intellectual property (IP), technology transfer contractual duties, electronic records management best practices, tort and criminal law and fiduciary duties. These are hugely diverse and complex influences so a comprehensive treatment of their details is well beyond the scope of this chapter. Nevertheless, various exemplars of these sources are examined conceptually to provide insight into how public policy exerts pressure that constitutes a confluence of regulatory and market-based forces influencing the development, implementation, testing, revision and evolution of internal control. These pressures comprise a major component of the public policy environment of IT Governance. In the U.S., privacy laws are apparently distinct regimes, so they may be misinterpreted as limited, "sectoral" silos applicable only narrowly to particular industries or professions. However, this chapter argues that they are increasingly broadening to include internal control pressures impacting service providers, consultants, publicly-traded corporations, closely-held companies, non-governmental organizations (NGOs) and government agencies at all levels (Bagby, 2007-2).

This chapter proposes a supply chain analysis that should apply to the data flows of information but that is not dependant on any supply chain in goods or services. Supply chain concepts and network analysis is adapted to information data flows starting from the acquisition of PII, through the archiving and processing of PII, to analysis