Chapter 11
Data Breach Disclosure:
A Policy Analysis

Melissa J. Dark
Purdue University, USA

ABSTRACT

As information technology has become more ubiquitous and pervasive, assurance and security concerns have escalated; in response, we have seen noticeable growth in public policy aimed at bolstering cybertrust. With this growth in public policy, questions regarding the effectiveness of these policies arise. This chapter focuses on policy analysis of the state data breach disclosure laws recently enacted in the United States. The state data breach disclosure laws were chosen for policy analysis for three reasons: the rapid policy growth (the United States have enacted 45 state laws in 6 years); this is the first instantiation of informational regulation for information security; and the importance of these laws to identity theft and privacy. The chapter begins with a brief history in order to provide context. Then, this chapter examines the way in which historical, political and institutional factors have shaped our current data breach disclosure policies, focusing on discovering how patterns of interaction influenced the legislative outcomes we see today. Finally, this chapter considers: action that may result from these policies; the action type(s) being targeted; alternatives that are being considered, and; potential outcomes of the existing and proposed alternative policies.

INTRODUCTION

Although advances in computing promise substantial benefits for individuals and society, trust in computing and communications is critical in order to realize such benefits. The hope for cybertrust is a society where trust enables technologies to support individual and societal needs without violating confidences and exacerbating public risks. Cybertrust, in part, depends upon software and hardware technologies upon which people can justifiably rely. However, the cybertrust vision requires looking beyond technical controls to consider how other forms of social control

DOI: 10.4018/978-1-61692-245-0.ch011

contribute to the state of cyber trust. This chapter focuses on public policy. While the chapter does not specifically use the word *ethics*, it should be noted that ethical issues and public policy are intimately intertwined. Policy is not formed in a moral vacuum; on the contrary, policy is inherently normative in that it prescribes, sometimes explicitly and often implicitly, what *should be*.

The increased reliance on and utilization of information technology in society has created the need for new regulation regarding the use and abuse of these systems. We see this clearly just by briefly inventorying some of the regulations that have been enacted to protect security and privacy.

- Freedom of Information Act (1966)
- Fair Credit Reporting Act (1970)
- Bank Secrecy Act (1970)
- Privacy Act (1974)
- Family Educational Rights and Privacy Act (FERPA) (1974)
- Right to Financial Privacy Act (1978)
- Foreign Intelligence Surveillance Act (1978)
- Electronic Communications Privacy Act (ECPA) (1986)
- Telephone Consumer Protection Act (1991)
- Communications Assistance for Law Enforcement Act (1994)
- Driver's Privacy Protection Act (1994)
- Health Insurance Portability and Accountability Act (HIPAA) (1996)
- Computer Fraud & Abuse Act (1996)
- Children's Online Privacy Protection Act (COPPA) (1998)
- Digital Millennium Copyright Act (1998)
- Gramm-Leach-Bliley Act (GLBA) (1999)
- USA PATRIOT Act (2001)
- Federal Information Security Management Act (2002)
- Fair and Accurate Credit Transactions Act (2003)
- CAN-SPAM Act (2003)
- 45 State Data Breach Disclosure Laws[1] law (2003-present)

Eight of these laws were enacted between 1966 and 1986, while the last thirteen items in the list have been enacted between 1991 and 2009. This is not an exhaustive list, but it is representative and shows the increasing growth in legislation. This chapter focuses on the 45 State Data Breach Disclosure laws enacted in United States between 2003-2009 – a mere six year time span. Data breach has become a policy concern due to the rise in identity theft crimes and the erosion of privacy.

Identity theft is the crime of obtaining and using another person's personal information in order to commit fraud. There are four types of identity theft: (1) financial – illegally using someone else's identity to obtain good and services, (2) criminal – posing as another person when apprehended for a crime, (3) identity cloning – using another person's information to assume his/her identity in daily life, and (4) business/commercial identity theft – using another business' name to obtain credit (Identity Theft Resource Center, 2008). Identity theft is a concern because of the escalating incidence and costs for individuals, companies, and our nation. It is estimated that there were 8.4 million U.S. adult victims of identity fraud in 2007 resulting in losses of $49.3 billion (Javelin Strategy and Research Survey, 2007). A study by the Ponemon Institute (2008) surveyed 35 U.S. organizations and found the total average cost of a data breach in 2007 was $202.00 per record breached. The Privacy Rights Clearinghouse maintains a chronology of data breaches (www.privacyrights.org) that includes data elements considered useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. According to this chronology, there were approximately 34,000,000 records breached in 2008 in the United States.[2] If the number of records breached and costs per breach in 2009 are commensurate with the 2008 costs, the estimated costs for data breaches 2009 will be $6,868,000,000 ($197 x