



Chapter X

Out of Control? The Real ID Act of 2005

Todd Loendorf, North Carolina State University, USA

Abstract

The tragic events of September 11, 2001, created an environment that was conducive to the expansion of surveillance operations. Furthermore, the Bush Administration's belief that the power of the presidency allows for any action, in the name of national security, led to the gathering of information about both terrorists and ordinary citizens. The Real ID Act of 2005 is a piece of legislation that requires, among other things, that state licensing agencies verify, collect, store, and share an increased amount of personal information. Opponents of this legislation are concerned about the financial, technological, privacy, and security implications of a law that was enacted with little to no due diligence. Currently, the requirements of the Real ID Act have been forced into an immigration bill in the Senate. Fortunately for those opposed to the Real ID Act, the Democratic majority currently in Congress appear to be more concerned with protecting the freedoms and liberties of American citizens than the Republican majority was when they originally passed the Real ID Act legislation in 2005. Ultimately, this chapter seeks to provide the reader with a thorough discussion into the many concerns associated with the Real ID Act.

Introduction

Daniel Webster once said “that good intentions will always be pleaded for every assumption of authority. It is hardly too strong to say that the Constitution was made to guard the people against the dangers of good intentions.” In a day and age when a majority of Americans seem willing to trade personal liberties for the prospect of security, it is important to remember the words of Webster. Certainly, the terrible events of 9/11 contributed to the willingness of a nation to turn a deaf ear to Webster and other protectors of personal liberty. This is a logical reaction to a very tragic sequence of events as we all tend to become more conservative and seek safety when we are threatened (Maslow, 1943). Unfortunately, a major problem in America today is that some would have us believe that our personal safety is at risk around every corner and in every facet of our daily life. In fact, security concerns fuel a multibillion dollar industry for everything from car alarms to home protection systems to Internet virus protection. Some might say that, as a society, we are more scared and less free than our rhetoric might suggest.

This growing culture of fear has provided ample opportunity for those determined to engineer safety through increased control. Examples of new age controls for safety are everywhere. Red light cameras, parking lot cameras, employee badges and background checks, antivirus software, and biometric scanners are a few of the ways we have created to protect our safety. To be clear, these measures are not the problem. In fact, they can do a lot of good. The problem lies in the way in which the information collected by these devices is so easily mismanaged.

In February 2007, 1,400 members of the California National Guard found this out the hard way. A computer hard drive containing Social Security numbers, home addresses, birth dates, and other identifying information of these troops deployed to the U.S.-Mexico border was stolen on February 23, 2007. Considering the sensitive nature of the work performed by these troops, a breach in the safety of their personal information is unacceptable. Furthermore, it casts a very dark cloud over any attempts to collect and store personal information. This is especially true considering this breach came on the heels of another security infraction in the military community in California. In January 2006, a report containing the names and Social Security numbers of more than 1,000 high-ranking California National Guard officers was in a briefcase stolen from a car in Sacramento. Unfortunately, the issues surrounding mismanaged data and the security of personal information are not contained to the military community in California. In fact, the issues are propagating throughout our society at an alarming rate despite the increasing awareness about the importance of information security. For this reason, we must heed the sage advice given to us by Webster over 200 years ago and carefully consider the impacts associated with any attempt to collect and store personal information in the name of security.

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/out-control-real-act-2005/28022

Related Content

Antecedents to the Adoption of Digital Marketing by Start-Ups Under Startup-India and E-Governance Initiatives: A BRT Perspective

Nilesh Tejrao Kate, Prashant Chaudhary, Kumod Kumar, Neelam Rautand Mahendra More (2024). *International Journal of Electronic Government Research* (pp. 1-23). www.irma-international.org/article/antecedents-to-the-adoption-of-digital-marketing-by-start-ups-under-startup-india-and-e-governance-initiatives/347505

Implications of e-Government in Botswana in the Realm of e-Participation: Case of Francistown

Vako Mbako, Kelvin Joseph Bwalya, Tanya Du Plessisand Chris Rensleigh (2012). *Active Citizen Participation in E-Government: A Global Perspective* (pp. 276-295). www.irma-international.org/chapter/implications-government-botswana-realm-participation/63375

Blockchain Use Cases in Healthcare

Alaattin Parlakklç (2022). *Blockchain Technologies and Applications for Digital Governance* (pp. 85-104). www.irma-international.org/chapter/blockchain-use-cases-in-healthcare/293836

Open Source in Government

David Berry (2008). *Electronic Government: Concepts, Methodologies, Tools, and Applications* (pp. 1171-1176). www.irma-international.org/chapter/open-source-government/9773

An Empirical Analysis of the Government Cloud Adoption in India

Kshitij Kushagraand Sanjay Dhingra (2021). *International Journal of Electronic Government Research* (pp. 21-43). www.irma-international.org/article/an-empirical-analysis-of-the-government-cloud-adoption-in-india/283070