Chapter 4.15
U.S. Federal Data Mining Programs in the Context of the War on Terror:
The Congress, Court, and Concerns for Privacy Protection

Shahid M. Shahidullah
Virginia State University, USA

Mokerrom Hossain
Virginia State University, USA

ABSTRACT

This chapter examines the issues and concerns raised in the context of the recent growth of federal mining programs. The chapter argues that in the context of the war on terror, intelligence gathering on terrorist activities both within and outside the United States has emerged as one of the core strategies for homeland security. The major national security related federal agencies such as the Department of Justice, Department of Homeland Security, and the Department of Defense have developed a number of data mining programs to improve terrorism intelligence gathering and analysis in the wake of the events of September 11, 2001. Some data mining programs have, however, raised a number of issues related to privacy protections and civil liberties. These issues have given birth to a wider debate in the nation and raised new tensions about how to search for a balance between the needs for the protection of privacy and civil liberties, and the needs for national security. The authors believe that the future of this debate is intimately connected to the future of the war on terror. Currently, Congress and the federal courts seem to be more in favor of supporting the preeminent needs of protecting national security. Through a number of enactments, Congress has broadened the federal power for collecting terrorism intelligence

DOI: 10.4018/978-1-61350-323-2.ch4.15

both at home and abroad. In a number of cases, the federal courts have ruled in favor of the doctrines of the "state secret privilege" and the "inherent power of the President" to emphasize the overriding need for protecting national security in the context of the war on terror. As America has embarked on a long and protracted ideological war against radical militant Islam, issues of national security and the need for data mining for detecting and analyzing terrorist activities are likely to remain dominant for a long time.

INTRODUCTION

The birth of the computer and the Internet, and the rise of the information revolution have brought some fundamental transformations in the way information can be created, organized, analyzed, stored, and shared. A new generation of information technology has emerged today that made us able to gather an unfathomable amount of data about the mysteries of the space and the galaxies, the baffling nature of the earth and the seas, and the complexities of the human bodies, brains, minds, and behavior. The everyday life in the information society is a bundle of digital texts, bits, and bytes that can travel through space and time without much control of those who own and produce them. In our everyday life, we participate in the digital economy and roam around cyber space with the computer sitting in the privacy of our home and family (Tapscott, 1999). The unseen and the boundless cyber space, however, knows no privacy. Our information in cyber space is virtually opened to the world, and it is irretrievable. Through our participations in the digital economy and our use of the Internet, we create a series of virtual data structures about our daily activities—our work, education, health, home, travel, and entertainment. These data structures remain stored in various places such as telephone companies, Internet service providers, banks, credit card companies, hotels, airlines, travel agencies, and tourist organizations. Information scientists describe data warehousing as the process of organizing and storing data structures. By creating these data structures, we, in fact, create a digital profile of our habits, choices, preferences, and prejudices. Through these data structures, one can even glean through the profiles of our families, friends, and relatives who live across different regions and countries. These data structures can lead to the discoveries of our habits and identities. They can lead to the discoveries of our patterns of thoughts, beliefs, and associations. Information technology or the methodology that makes these analyses and discoveries possible is known as data mining.

Data mining has opened up a new horizon of possibilities for growth and expansion in information science, artificial intelligence, supercomputing, human genetics, neurology, medicine, earth science, and many other areas of scientific research (McCue, 2006; Wang, 2005). A variety of marketing, advertising, and business organizations today use data mining to create profiles of the habits and preference of their consumers (Perner, 2002). The use of data mining by business organizations and governmental agencies, however, has raised a number ethical and moral questions related to privacy, democracy, and civil liberties.

A debate is currently growing in America about the use of data mining by many federal agencies, particularly about the ones that are being conducted in the context of the war on terror. Federal agencies working with national security and homeland protections find in data mining a new weapon of intelligence to combat and prevent terrorist activities both within and outside the United States. In the larger society, however, concerns are being raised about how federal data mining programs undermine the notions of privacy and civil liberties (Carafano,, 2007; DeRosa, 2004; Heymann & Kayyem, 2005; United States