Chapter XV
International Outsourcing, Personal Data, and Cyber Terrorism:
Approaches for Oversight

Kirk St.Amant
Texas Tech University, USA

ABSTRACT

An individual's personal information can be a valuable commodity to terrorists. With such data, terrorists can engage in a variety of illicit activities including creating false bank accounts, procuring various official documents or even creating mass panic. Unfortunately, such personal data is generally easy to access, exchange, or collect via online media including Web sites, chat rooms, or e-mails. Moreover, certain common business practices, particularly those related to data processing in international outsourcing, can facilitate such activities by placing personal information into a legal grey area that makes it easy to misuse. For these reasons, organizations and individuals need to be aware of the potential for such data misuse as well as be informed of steps they can take to curtail such abuses. This essay examines the privacy/data abuse problems related to international outsourcing and presents approaches designed to prevent the misuse of personal information by cyber terrorists.

INTRODUCTION

An individual's personal information can be a valuable commodity to terrorists. With such data, terrorists can set up false addresses for receiving materials, establish unknown lines of credit, apply for visas, passports, or other documents, or siphon money from bank accounts (Lormel, 2002; Sullivan, 2004). On a large scale, terrorists can misuse personal data in ways that could cause mass panic; crash an organization's or a region's computer systems, or spread misinformation throughout a community (Lormel, 2002; Sullivan,

2004). For these reasons, the protection of personal information is of paramount importance to combating terrorism.

Unfortunately, such data is often freely exchanged and easily compiled via online media such as Web sites, chat rooms, or e-mails. As a result, personal information can be a prime and easy target for *cyber terrorists*—or individuals who use online media to engage in or enable terrorist activities. Moreover, certain business practices actually place large amounts of personal data into an environment where it can easily be abused by others.

One of the more problematic of these practices is international outsourcing. By moving personal data beyond the reach of certain authorities, international outsourcing activities can facilitate the uses of personal data for nefarious ends. This chapter examines privacy and data abuse problems related to international outsourcing. It also presents approaches organizations can use to prevent the misuse of personal data by cyber terrorists.

BACKGROUND

When organizations outsource, they allow other individuals or companies to perform work for them (Bendor-Samuel, 2004). The decision to outsource usually involves two factors: cost and efficiency. That is, client businesses outsource tasks to organizations that can perform them more cheaply and efficiently than the client business can. Such work, moreover, is often outsourced to persons or organizations located in other nations—a process known as *international outsourcing* or *offshoring*.

While companies have been sending manufacturing work overseas for some time, the nature of the work being outsourced now includes a wide range of knowledge-based tasks including information technology (IT) management, software and video game programming, accounting, and medical transcription. In many cases, companies based in North America and Western Europe export work to outsourcing providers located in developing nations such as India, China, and the Philippines.

The benefits associated with such offshoring practices have led to an explosion in this industry. Today, international outsourcing is worth some $10 billion and accounts for almost 500,000 jobs in India alone (Baily & Farrell, 2004; Rosenthal, 2004b). These situations might be the tip of a growing outsourcing iceberg, for certain observers claim the international outsourcing market will grow 20% a year through 2008 and account for three to five million knowledge-based jobs by the middle of the next decade (Baily & Farrell, 2004; Garten, 2004; Rosenthal, 2004b). This expansion will also mean outsourcing providers will arise in a wider range of developing nations as workers in Eastern Europe, Asia, South America, and Africa try to tap into this lucrative service market (Reuters, July 18, 2004; Rosenthal, 2004a; Rosenthal, 2004c).

This growth in outsourcing, moreover, will involve a wider range of knowledge-based work, particularly in the areas of financial processing and medial care. As a result, more sensitive information will move overseas to facilitate these activities. Such trends, however, create new legal situations related to data collection and distribution. By using more than one nation in a data processing activity, offshoring involves more than one legal system in the regulatory process.

The problem involves the legal concept of jurisdiction, or when a particular law can and cannot be enforced. According to this idea, the laws of one nation are often only enforceable within its borders. Thus, once individuals or materials move beyond those borders, they are generally beyond the legal protection of that nation.

Offshoring creates an interesting jurisdiction situation. If work is performed in another nation, then employees might be operating under a set of laws that is quite different from those that govern the company that provided the work. Therefore, a process that might be an illegal—or black market—activity in the nation of the outsourcing client could be a legal—or white market—one in the nation where the outsourcing employee resides. This situation is particularly problematic in relation to the protection of personal information, for the national laws dealing with this issue vary from the strict (e.g., European Union's Data Protection Directive) to almost non-existent (e.g., the