Chapter 7.3
Grey Market Informatics

Kirk St.Amant
East Carolina University, USA

INTRODUCTION

International outsourcing often involves virtual communities in which globally dispersed co-workers use online media to collaborate on projects. Such virtual work communities are associated with reduced production costs and quicker times to market. These work relationships, however, also bring with them certain detriments. While critics have focused on job losses related to international outsourcing, few individuals have examined outsourcing's other great drawback: diminished control over information. This reduced control creates an opening for the misuse of personal data through a series of processes collectively referred to as *grey market informatics*.

This article overviews how grey market informatics works and examines the effects it can have on organizations that use international outsourcing. The article then concludes with strategies for avoiding such misuses of data. By realizing and addressing grey market informatics, organizations can enhance the success of their future outsourcing activities.

BACKGROUND

International outsourcing increasingly involves the export of sensitive personal data to overseas workers who process it. For example, the outsourcing of accounting practices moves financial data beyond the legal protections of the client nation (e.g., the United States [U.S.]) (Relocating the back office, 2003; Lost in translation, 2003). Similarly, more confidential medical information is moving abroad as processes such as medical transcription are outsourced (Davino, 2004).

By moving information from one nation to another, these outsourcing practices shift such data into a legal grey zone. While the outsourcing client (the *client organization*) might be located

in a nation where laws prevent such data from being abused, that same information might be outsourced to a nation where no such legal protections exist. As a result, international outsourcing can leave personal information vulnerable to various abuses.

To appreciate this vulnerability, one needs to understand the role personal data plays in marketing and development practices. Effective marketing is based on understanding consumers, and the more one knows about an individual, the easier it is to create advertising materials that entice that person to purchase a product. Personal data, therefore, is an important commodity, for it can be used to improve product sales. Corporations, in turn, often collect and archive as much personal data on individuals as possible, even if such personal data seemingly has no value related to marketing. The idea is that such information might have value later (Whitaker, 1999; Siebel & House, 1999; Davis & Meyer, 1998). Such data can also help organizations better plan research and development activities to meet purchasing patterns within a population and thus maximize the profits they can make from a product. If, for example, a pharmaceutical company knows more individuals suffer from heart disease than stomach disorders, it can focus drug development efforts on medications designed for the larger market.

Historically, the usefulness of personal data remained limited, for mass media (e.g., television, radio and print advertising) served as the primary means for sharing advertising with consumers. Advertising, therefore, had to address a broad, general audience in the hopes that the related message would persuade enough consumers to purchase a product. Online media changed marketing by allowing marketers to deliver advertising directly to specific consumers. This direct contact means advertising can now be designed to meet the interests of specific individuals. Such narrowcast advertising permits organizations to use more personalized marketing to increase sales one customer at a time.

Additionally, this ability to focus on individuals also facilitates the sales of specific goods and services to consumers who seemed most likely to purchase them. It also provides organizations with a database of valuable data that others might be willing to purchase. As a result, the value of personal information has skyrocketed, and so has the business imperative to collect as much of this information as possible (Whitaker, 1999; Siebel & House, 1999; Davis & Meyer, 1998).

These trends in data collection have also given rise to consumer concerns related to misuses of personal data. Insurance companies, for example, could rely on data a pharmaceutical company uses to target a blood pressure drug to a prospective consumer to deny coverage to the same individual. These privacy concerns have prompted many governments to enact laws that protect consumer information. In the U.S., for example, the Fair Credit Reporting Act and the Credit Reporting Reform Act place restrictions on how an individual's financial data may be used (Cate, 1997). Similarly, the Cable Communications Policy Act and the Video Privacy Protection Act greatly limit how organizations use data related to consumer purchase or rental patterns (Cate, 1997). More recently, the Electronic Communication Privacy Act has established privacy protections related to computer use (e.g., keystroke monitoring) and online communication (e.g., "rerouting electronic communications to provide contemporaneous acquisition") (Johnston, Handa, & Morgan, 1997, p. 81). For these reasons, organizations must often perform a complicated balancing act related to consumer privacy. On the one hand, they have a vested interest in compiling and using consumer data. On the other, legal guidelines restrict their abilities to perform such processes.

Historically, this balance was kept due to limitations in the geography of the workplace. That is, organizations usually performed their data processing activities within the borders of a particular nation. As a result, the organizations performing such activities had to comply with