Grey Market Informatics

Kirk St. Amant
Texas Tech 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 Re-
Grey Market Informatics

porting 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 privacy laws of its “home nation.” This geographic restriction meant violations were relatively easy to track and penalties were relatively easy to enforce. The international access provided by online media altered the geography of the workplace and affected the nature of privacy protection related to corporate activities.

Global use of online media has grown markedly in recent years, and much of this growth is taking place in developing nations. In mainland China, the number of Internet users grew from 2.1 million in 1999 to a projected 96 million by the end of 2004, while Brazil has seen its number of online users grow by 430,000 in recent months (Wired China, 2000; China’s coming, 2004; Active Internet users August, 2004). Now, employees located in different nations can use these media to communicate as quickly and effectively as if they were working within the same building. As a result, work groups have shifted to virtual communities comprised of employees based in various countries (Relocating the back office, 2003; Lost in translation, 2003). These virtual communities often involve international outsourcing—a process by which organizations send work overseas and monitor production from a distance.

Online-based outsourcing brings with it the prospect of increased profits for two reasons. First, online media allow companies to use knowledge workers in developing nations to perform skilled tasks for a fraction of what employees in industrialized nations would charge (The new geography, 2003). Second, online media either allow individuals in different nations to work on the same project simultaneously or to forward work from nation to nation in order to keep production going non-stop (Friedman, 1999). Such processes reduce the time it takes to generate final products and get them into the marketplace.

International outsourcing also creates interesting legal situations. If work is performed in another nation, then employees are operating under laws different from the company that provided the work. Therefore, a process that might be illegal in the nation of the outsourcing client might be perfectly legal in the nation of the outsourcing employees. In terms of privacy and data protection, the various national laws dealing with such topics can range from very strict (e.g., the European Union’s Data Protection Directive) to almost non-existent (e.g., Pakistan) (Swire & Litan, 1998). The result is a grey area in international law; which laws should apply where and how? Within this grey area, a field of data collection could emerge: that of grey market informatics.

MAIN THRUST

Grey market informatics is a process in which differences in national privacy laws allow personal data to be used in questionable ways—many of which focus on profits. In some cases, international outsourcing could be used for purposes of data laundering. In these situations, a client organization is located in a nation that has laws restricting how personal information can be compiled into a consumer profile for marketing or research purposes. Organizations might therefore outsource personal information to nations where such data compiling is legal. Outsourcing employees could send these profiles to a subcontractor—a different individual located in that same nation or located in another nation with lax privacy laws. That subcontractor would return profiles to the original client organization. As that client organization did not violate its own nation’s laws, it could use the resulting profiles in its marketing or development activities.

In other cases, national laws might make it illegal for organizations to receive profiles created from “illegally compiled data.” Again, grey market informatics allows organizations to circumvent such laws. This time, once marketing profiles are created by overseas workers, those profiles are not returned to the client organization. Rather, they are sent to a different organization (an outsourced subcontractor) that would use the data in marketing activities on behalf of the original client organization. In this way, the client organization does not violate the laws of its own nation, but it can still reap the benefits of using specific consumer information. Such scenarios could be viewed as indirect applications of data.

In both instances, the benefit of grey market informatics has to do with tracking and punishing violations. Once information is sent beyond the borders of a particular nation, that nation’s regulatory agencies might not be