Dataveillance and Panoptic Marketspaces

Nikhilesh Dholakia  
*University of Rhode Island, USA*

Detlev Zwick  
*York University, Canada*

Anil Pandya  
*Northeastern Illinois University, USA*

**ELECTRONIC MARKETS**

With continuing global growth of electronic commerce, consumers have come to exist in electronic “marketspaces” (Rayport & Sviokla, 1994) that are frequently surveilled through database techniques. This type of data-driven monitoring has been characterized as “dataveillance.”

This article reviews the main characteristics of such dataveilled and panoptic marketspaces, from the perspectives of critical social theories.

**EXAMPLES OF DATAVEILLED MARKETSPACES**

The term *dataveillance* is attributed to Australian computer scientist Roger Clarke (1988). Apart from the technically informed critiques by Clarke, the virtual dataspaces intersecting with human bodies have been discussed by Kroker and Weinstein (1994) and the condition of humans located in database matrices has been critiqued by Poster (1990a, 1995a). Aspects of dataveillance in e-commerce and m-commerce marketspaces have been addressed by Dholakia and Zwick (2001) and Zwick and Dholakia (2004).

What do the emergent dataveilled marketspaces look and feel like? We provide short descriptive cases to illustrate them.

**JetBlue Passengers Face the Blues**

The U.S. Department of Defense carried out a project to identify potential terrorists among airline passengers who could possibly attack army bases. Ordinary airline passengers became the unwitting pawns in this data-invasion exercise. In September, 2002, Torch Concepts—a data mining firm on contract from the army—acquired from JetBlue Airways (a discount air carrier) the itinerary data for over 1.5 million passengers, including passenger names, addresses, and phone numbers. Of these passenger records, 40% were cross-referenced with gender, home specifics (owner/renter, etc.), years at residence, economic status (income, etc.), number of children, Social Security number, number of adults, occupation, and vehicle information—detailed demographic data obtained from a database vendor. While this substantial panoptic exercise—undertaken without any knowledge or consent of the passengers concerned and in violation of JetBlue Airways declared privacy policies—found only one possible anomalous passenger record, the potential for massive invasion of marketspace data records is quite evident in this case (EPIC, 2003).

**Do the Insured Have a Clue?**

Michael Ha of National Underwriter is worried that when massive databases such as the Department of Motor Vehicles (DMV) records and Comprehensive Loss Underwriting Exchange (CLUE) cross-reference each other, insurance companies can benefit at the expense of clueless drivers. Although such databases have legitimate uses, such as determining insurance premium rates for motorists, they can also be misused. Blending such private data with data collected from emerging technologies such as event recorders and global positioning systems, these systems are capable of generating real-time data profiles of drivers, in effect providing insurers a secretive “eye in the sky” to monitor drivers. When such data is married with information in massive DMV and CLUE databases, serious privacy concerns arise. Some insurance companies are encouraging automobile makers to install monitoring technologies in high-end vehicles. Ethical boundaries are being crossed, however. Allstate, a major insurer, has already paid $1 million to the California DMV in settlement of a dispute about unethical use of DMV records (Ha, 2003).
Your CEO Wants You to Do This

If you are assisting your CEO with forecasting tasks, how would you react to a personalized letter, such as this from a software maker:

Mr. P [actual name of your CEO] is interested in this product. What would it be worth to Mr. P if you increase the accuracy of your decisions by 10%? How about 25%? What if you double your effectiveness? Although the future is difficult to foresee, I predict your next “What-If” analysis will result in better insights. Your superiors such as Mr. P will place more confidence in your analysis. You’ll make better decisions. (Brent Green & Associates, 2003)

Such a letter was sent by database marketing firm Brent Green & Associates (BGA) on behalf of the software firm making the forecasting product. The letter was “signed” by the president of this software firm, and BGA selected a list of subscribers to a well-known newsletter targeting financial planners, security investment advisors, security analysts, and brokers. Then BGA matched each prospect on the first list with another list containing names of company presidents obtained from American Business Information, which also included company details. Based on such matched names, each prospect received a letter from BGA bearing the message portrayed above. Some of the letter recipients were enraged at this invasion of privacy, and the president of BGA received a few flaming telephone calls. One caller was livid and threatened to notify the Better Business Bureau and promised that his bank would never buy software from this company. Thus, BGA learned that marrying two or more databases is risky, even if creative overlays offer tempting ways to grab attention (Brent Green & Associates, 2003).

Have You Refilled Your Prescription?

Rite Aid Pharmacy wrote a letter, sponsored by a pharmaceutical manufacturer, to Lisa in California to “remind” her to refill a particular prescription medication that she was taking. Shortly thereafter, Rite Aid called her husband to “remind” him to refill a particular prescription medication that he was taking. The woman felt that Rite Aid was using her prescription records and her family’s private medical information to aggressively market prescription medications. She considered the conduct of Rite Aid unprofessional and complained to the California Department of Consumer Affairs (Privacy Rights Clearinghouse, 1999).

PRIVACY-PERMISSION DYNAMICS

With increased dataveillance comes increasingly data-intrusive marketing techniques, such as spam e-mail. Publicly accessible databases and data streams might be easily harvested by aggressive spammers, often for unscrupulous use. In the deluge of unwanted spam and pop-up windows, legitimate and desired marketing interactions could get sidelined. Permission marketing (Godin, 1999), with its very tightly specified “opt-in” e-communication parameters, and e-commerce Web sites, with strong privacy policies, are belated responses to such developments.

In principle, permissions-based e-commerce seems to take care of privacy invasion problems. In practice, things are more complex. In the evolving privacy-permission dynamics in electronic marketspaces, several contentious issues remain. For example,

- Opt-out permission methods, capable of confusing all but the most vigilant consumers, are used far more frequently than consumer-friendly opt-in methods.
- The scope of permission—its breadth and depth—is often unclear, and companies can take advantage of this by interpreting permissions in broader and deeper ways that favor them rather than the consumers.
- It is unclear whether permission granted by the customer to a marketer is transferable to a third party that acquires the customer’s information from the marketer.
- Customer permission is very business-specific. What happens if the business is acquired and the customer does not want to grant permission to the acquiring company?
- Conversely, opt-out decisions may not be honored by the new owner of the original customer database, thus invalidating the customer’s initial decision.

CRITICAL SOCIAL THEORY PERSPECTIVES

Inspired by philosopher of technology Mark Poster (1990b; 1995b), we develop a poststructuralist critique of customer database technology. This approach construes information technology such as databases as configurations of language that produce new and signifi-