E-Technology Challenges to Information Privacy

Edward J. Szewczak
Canisius College, USA

INTRODUCTION

The collection of personal information by electronic technology (e-technology) and the possibility of misuse of that information are primary reasons why people limit their use of the Internet and are even limiting the success of e-commerce (Szewczak, 2004). Various uses of e-technology that collect and/or disseminate personal information include corporate and government databases, e-mail, wireless communications, clickstream tracking, and PC software. The main challenge to personal information privacy is *the surreptitious monitoring of user behavior on the Internet without the user's consent and the possible misuse of the collected information resulting in financial and personal harm to the user*. Our focus is primarily on Internet use in the United States of America, though clearly e-technology is global in nature and poses challenges and issues for societies around the world.

BACKGROUND

Concerns about the collection of personal information are ongoing. The results of a 1998 survey conducted by Louis Harris & Associates, Inc. revealed that worries about protecting personal information ranked as the top reason people generally are avoiding the Web (Hammonds, 1998). The misuse of credit card data for activities such as identity theft is a major concern (Stop thieves from stealing you, 2003; www.Truste.org/articles/holiday_shopping.php). A survey of 1068 consumers conducted by primary monitor Truste found that many people were skeptical of giving their personal information to online businesses. Seventy-five percent of respondents reported not liking to register at Web sites they visit. Fifteen percent of respondents refused to register at all. Forty-three percent of respondents stated they did not trust companies to not share their personal information. Of those respondents who did share personal information, 25% said they were less than impressed with the return on the information they provided (www.Truste.org/articles/quarterly_index1.php). A 2005 California HealthCare Foundation and the Health Privacy Project Poll found that 67% of national respondents are concerned about the privacy of their personal medical records (www.epic.org/privacy/medical/polls.html).

Dhillon and Moores (2001) reported that the selling of personal information by companies to third parties was the top privacy issue as identified by IS executives. However, failed Internet companies such as Boo.com, Toysmart.com, and CraftShop.com have either sold or have tried to sell customer data that may include phone numbers, credit card numbers, home address, and statistics on shopping habits, even though they had previously met Internet privacy monitor Truste's criteria for safeguarding customer information privacy. The rationale for the selling was to appease creditors (Sandoval, 2000). Even financially healthy companies realize there are advantages to be gained in the selling of collected customer information. Buyers include other businesses as well as the U.S. government. The Departments of Justice, State, and Homeland Security spend millions of dollars annually to buy commercial databases that track American citizens' finances, phone numbers, and biographical data. Often these data are accepted at face value without further evaluation for accuracy (Woellent & Kopecki, 2006). Companies such as Amazon, Ebay, and Google have opened up access to their databases to other companies for free in hopes these companies will develop new products and services that are organized around their database systems (Schonfeld, 2005).

In his excellent study on privacy in the information age, Cate (1997) adopted the definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" from Westin (1967, p. 7). Westin/Cate's definition is interesting because it allows for flexibility in discussing privacy within the context of the Internet. Whereas many people worry about divulging personal information electronically, other people seem more than willing to give it away, trading their personal information for personal benefits such as free shipping and coupons (Kuchinskas, 2000). Personalized service is the main benefit. A Web site can save a shopper time and money by storing and recalling a user's tastes and buying habits (Baig, Stepanek, & Gross, 1999). ISPs are willing to allow Web users cheaper access to the Internet provided the users are amenable to having their online behavior tracked for marketing purposes by specialized software (Angwin, 2000). If users are not amenable to having their personal information shared among company subsidiaries, at least one company

has warned that discounts for offerings such as high-speed Internet service will be taken away (Lazarus, 2004).

TECHNOLOGICAL CHALLENGES TO PRIVACY

Corporate and Government Databases

The practice of gathering personal information about customers and citizens by corporations and governments is well established. Software is available that is dedicated to analyzing data collected by company Web sites, direct-mail operations, customer service, retail stores, and field sales. Web analysis and marketing software enable Web companies to take data about customers stored in large databases and offer these customers merchandise based on past buying behavior, either actual or inferred. It also enables targeted marketing to individuals using e-mail. Governments routinely collect personal information from official records of births, deaths, marriages, divorces, property sales, business licenses, legal proceedings, and driving records. Many of the databases containing this information are going online (Bott, 2000).

These company and government databases are often not adequately secure against various threats to their integrity. Companies such as Choicepoint, Bank of America, Time Warner, Acxiom, and CardSystems Solutions have experienced breaches of security wherein unauthorized access of customer information such as names, addresses, Social Security numbers, credit and debit card numbers, and driver's license numbers occurred (Carrns, 2005; Perez & Brooks, 2005). Other companies blame checkout software that improperly stored credit card data for security breaches (Bank, 2005). For some companies, the threat to data security is internal rather than external (Yuan, 2005).

The deregulation of the financial services industry has made it possible for banks, insurance companies, and investment companies to begin working together to offer various financial products to consumers. Personal financial information that was kept separate before deregulation can now be aggregated. In fact the ability to mine customer data is one of the driving forces behind the creation of large financial conglomerates. Services can be offered to customers based on their information profiles. Large credit bureaus such as Equifax and Trans Union have traditionally been a source of information about a person's credit worthiness. Their databases contain information such as a person's age, address, and occupation. Credit bureaus have begun to sell personal information to retailers and other businesses (Big browser is watching you!, 2000). Some mutual fund companies have disclosed information such as customer name, home address, and account numbers on a U.S. government Web site in response to a Securities and Exchange Commission regulation, leaving customers vulnerable to identity theft and other crimes (Maremont, 2005).

Like personal financial information, medical information is for most people a very private matter. Despite this fact, there is a wealth of personal medical data in government and institutional databases. As *Consumer Reports* (Who knows your medical secrets, 2000, p. 23) notes, "[t]he federal government maintains electronic files of hundreds of millions of Medicare claims. And every state aggregates medical data on its inhabitants, including registries of births, deaths, immunizations, and communicable diseases. But most states go much further. Thirty-seven mandate collection of electronic records of every hospital discharge. Thirty-nine maintain registries of every newly diagnosed case of cancer. Most of these databases are available to any member of the public who asks for them and can operate the database software required to read and manipulate them."

Much of personal health information that is available to the public is volunteered by individuals themselves, by responding to 800 numbers, coupon offers, rebate offers, and Web site registration. Much of the information is included in commercial databases like Behavior-Bank sponsored by Experian, one of the world's largest direct-mail database companies. This information is sold to clients interested in categories of health problems, such as bladder control or high cholesterol.

E-Mail

In a survey of 840 U.S. companies, 60% said they use some type of software to monitor employees' e-mail activities (Tam, White, Wingfield, & Maher, 2005). Despite the fact that most companies had policies alerting employees that they were subject to monitoring, some had fired employees based on evidence collected during monitoring (Seglin, 2000). Hackers can also be a problem. Programs can be surreptitiously installed that monitor a user's keystrokes. The keystrokes can be sent across the Internet to a computer that logs everything that is typed for later use (Glass, 2000).

Employee's invasion of privacy claims have not been upheld in the United States courts, which argue that, since employers own the computer equipment, they can do whatever they want with it (McCarthy, 2000). However, use of Google's Gmail could present an information privacy issue of another sort. Gmail searches for certain words in a user's incoming messages, then displays text ads related to the words. There is a potential for many messages accumulated on Google's servers to be combined to produce a profile of an individual that could be accessed by, say, a government law enforcement agency or a criminal organization (Jesdanun, 2005; Wildstrom, 2004, 2006).