Information Privacy and E-Technologies

Edward J. Szewczak
Canisius College, USA

INTRODUCTION

The use of various e-technologies for e-commerce, e-government, and mobile commerce is characterized by the collection of personal information—both routinely as well as surreptitiously—and the possibility of misuse of that information. Various uses of e-technologies that collect or disseminate personal information include corporate and government databases, e-mail, and wireless communications. (For a discussion of clickstream tracking and spyware, hardware and software watermarks, and biometric devices, see Szewczak, 2005) The main challenge to personal information privacy is the surreptitious monitoring of user behavior without the user's consent and the possible misuse of the collected information resulting in financial and personal harm to the user. In light of this reality, people limit their use of e-technologies, even to the point of limiting the success of e-commerce (Szewczak, 2004). Our focus is primarily on e-technology 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. Also, in light of the 9/11 terrorist attacks on the World Trade Center and the Pentagon and the U.S. government's response to them, the issue of information privacy takes on a new urgency (for more information, see www.privacyinternational.org).

THE IMPORTANCE OF INFORMATION PRIVACY

The results of a 1998 survey conducted by Louis Harris & Associates, Inc., revealed that worries about protecting personal information ranked as the top reason why people are generally avoiding the Web (Hammonds, 1998). A survey by NFO Interactive (for more information, see www.nfoi.com) found that the safekeeping of online consumer personal information was the main reason people chose not to shop online.

Furthermore, TNS and TRUSTe's quarterly study of consumer attitudes and behaviors on privacy topics found that many Web users are skeptical of the necessity of giving their personal information to online businesses and do not like registering at Web sites they visit. Forty-three percent of those surveyed stated they did not trust companies to not share personal information (e.g., see www.TRUSTe.org/articles/quarterly_index1.php). The misuse of credit card data for activities such as identity theft is a major concern (Westin, 2003). Identity theft involves the surreptitious assumption of a person's identity to secure bank loans, credit cards, and mortgages in that person's name. Victims usually do not have to pay for credit card purchases made in their name, although they may be liable in thefts involving other types of loans. It can take months and years for innocent victims to restore their damaged credit histories. Some identity thieves assume the identities of whole companies, using an employer identification number to secure commercial loans, corporate leases, or expensive office products. The Federal Bureau of Investigation claims that many identity thefts originate in Russia, Romania, and West Africa (O'Brien, 2004b).

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). Selling customer data is in direct opposition to the top Internet privacy issue as identified by Dhillon and Moores (2001).

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" Westin (1967, p. 7). Westin's and Cate's definition is interesting, because it allows for flexibility in discussing privacy within the context of e-technologies. 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). Microsoft's Passport is designed to allow a user to visit many Web sites without reentering personal information at each site (Clark, 2001). Internet service providers 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). SBC Communications has told its customers that it will take away discounts for its popular offerings like high-speed Internet access if they choose not to have their personal information shared among the company's subsidiaries (Lazarus, 2004).

E-TECHNOLOGY CHALLENGES TO INFORMATION 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; Cropper, 2005). Personal information that were once stored in filing cabinets in attorneys' offices, hospitals and financial institutions can now be accessed with a click of a mouse (I. Armstrong, 2002).

Public records, however relevant for ensuring fairness in government action, may be accessed online to acquire personal information about a wide variety of topics including a person's lifestyle or sexual history which may be included in court documents (e.g., divorce decrees). The same is true for private medical records if an insurance holder sues over payment claims. The problem is compounded by the fact that counties have sold information in bulk to commercial companies that repackage it or resell it to other companies or to individuals (Leach, 2004). Although most states require information like Social Security numbers be concealed before documents are made available online, it is impractical and sometimes impossible to catch every instance (Ogles, 2004).

Internet service providers maintain archives of Internet message boards. Even users who adopt pseudonyms to protect their identities when expressing opinions may be identified through logs of Internet access, length of time online, time of day the Web was surfed, and credit card numbers used to shop (Bedell, 2001).

The deregulation of the financial services industry provided by the Gramm-Leach-Bliley Act (GLB) 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 sell personal information to retailers and other businesses (Westin, 2000a).

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* (Westin, 2000b, p. 23) noted:

> *The 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 available to the public is volunteered by individuals 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. The Medical Information Bureau (MIB) is a database of medical information shared by insurance companies. If a person has a medical condition that an insurance company considers significant, the company will report that information to the MIB, where medical conditions are represented by codes (for more information, see www.privacyrights.org).