Personal Information Privacy and Internet Technology

Edward J. Szewczak
Canisius College, USA

INTRODUCTION

Concerns about the collection of personal information by Internet technology and the possibility of misuse of that information are a primary reason why people limit their use of the Internet and are even limiting the success of e-commerce (Szewczak, 2004). Various uses of technology that collect and/or disseminate personal information include corporate and government databases, e-mail, wireless communications, clickstream tracking, hardware and software watermarks, and biometric devices. 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 the technology is global in nature and poses challenges and issues for societies around the world.

PERSONAL INFORMATION AND INTERNET USE

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). A survey by NFO Interactive (*www.nfoi.com*) found that the safekeeping of online consumer personal information was the main reason people chose not to shop online. The misuse of credit card data for activities such as identity theft is a major concern (*Consumer Reports,* 2003).

Some recent events serve to confirm these concerns. Italian Privacy Commissioner Stefano Rodota ordered Infostrada to temporarily shut down its free ISP service because it required users to disclose their age, health status, sexual habits and political, labor and religious preferences in order to qualify for the service. Infostrada said that the information was required for marketing purposes (*http://www.privacytimes.com/NewWebstories/oxymoron_prv_2_23.htm)*. 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). The Foundation for Taxpayer and Consumer Rights purchased the Social Security numbers and home addresses of the CIA director and the U.S. Attorney General on the Internet for $26 (Kerr, 2003).

WHAT IS PRIVACY?

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/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, Spepanek & 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). Spyware installs itself on computers when users download programs, and then tracks each click the user makes (Hagerty & Berman, 2003).

TECHNOLOGICAL CHALLENGES TO PRIVACY

Government regulators and enforcement officials have to consider a host of technological challenges to personal information privacy on the Internet.

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). MGM Mirage's online gambling business is aided by online screening programs wherein a bettor's location is determined using Internet mapping software and personal details checked against six external databases (King, 2003).

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 (*Consumer Reports,* 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* (2000b, p. 23) notes:

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 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

E-mail accounts for 70% of all network traffic, yet only 10% of it is protected by security measures. Thus it is susceptible to tampering and snooping (Armstrong, 2000; Weingarten & Weingarten, 2002). In many companies, employee e-mail communications are routinely monitored. Despite the fact that most companies had policies alerting employees that they were subject to monitoring, 25% surveyed 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).

Employees' 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).

Wireless Communications

Wireless advertising poses a host of challenges for privacy advocates. Wireless service providers know customers' names, cell phone numbers, home and/or office addresses, and the location from where a customer is calling as well as the number a customer is calling. Each phone has a unique identifier that can be used to record where in the physical world someone travels while using the cell phone (Petersen, 2000). The Federal Communications Commission requires cell phone service providers to be able to identify the location of a caller who dials 911, the emergency number. Since a cell phone service provider can track the location of a 911 call, it can track the location of any other call as well.

Clickstream Tracking

Tracking employee behavior on the Internet has become common practice. Software programs have been specifically designed to monitor when employees use the Internet and which sites they visit (McCarthy, 1999b).