

Oh, what a tangled web we weave: The state of privacy protection in the information economy and recommendations for governance

Jeff Langenderfer^{a,*}, Don Lloyd Cook^{b,1}

^a*Campbell School of Business, Berry College, Mount Berry, GA 30149, USA*

^b*Robinson College of Business, Georgia State University, Suite 1300 RCB, Atlanta, GA 30303, USA*

Abstract

The explosion of database marketing combined with the advent of computer matching programs and cheap computing power has forever changed the face of data collection and distribution in America and the world. Never before have marketers had such inexpensive access to reliable information about consumers. This new marketing power has, however, come with a privacy price tag that many consumers find objectionable: Detailed personal data on virtually every American is readily available for discovery or download at little or no cost. This relatively new state of data availability operates against a backdrop of limited privacy regulation. Federal privacy statutes largely focus on government distribution of information, not private data exchanges. State laws vary widely, with some states heavily regulating the type of information that can be exchanged and others providing few restrictions on private information distribution. The result is a significant series of gaps in the privacy protections for consumers. In this paper, we examine federal and state laws that restrict data collection and distribution in the United States and their strengths and weaknesses in the face of rapid technological advancement. We also develop a framework for classifying the existing privacy mechanisms. We use this framework to explore the implications for a comprehensive overhaul of the statutory privacy policy as well as the consequences of maintaining the status quo in an era in which the existing statutes are effectively overwhelmed by the changing technology.

© 2002 Elsevier Inc. All rights reserved.

Keywords: Privacy

1. Introduction

Of all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers, from the inspection and scrutiny of others. Without the enjoyment of this right, all others would lose half their value. (In re Pacific Railway Commission, 1887, p. 250)

You have zero privacy anyway. Get over it. (Scott McNealy, CEO Sun Microsystems, in Piller, 1999)

In the brave new online world that Americans now inhabit, data collection has become a state of the art practice. Internet sites collect information about visitors and track

their clicking through the use of cookies (McCune, 1999). Information brokers bundle records of every conceivable kind, selling and exchanging data packages for pennies per name or address. This information environment provides incredible marketing efficiencies, but also comes with a privacy price—reliable information about nearly every American is readily available for purchase or download (Beauprez, 1999).

One result of our data-rich domain has been a growing clamor for increased privacy protection (Safire, 1999; Thomasson, 1999), as only a patchwork of laws presently protect individual privacy interests (Gellman, 1993). As data collection has become cheaper and the tools for information management become more sophisticated, data collection has become a big business (see Avrahami v. US News and World Report, 1996). Internet and other direct marketers often use consumer data to focus their marketing efforts and, as consumer data collection techniques have improved, so have the quality and quantity of the informa-

* Corresponding author. Tel.: +1-706-238-5893; fax: +1-706-238-7854.

E-mail address: jlangenderfer@campbell.berry.edu (J. Langenderfer).

¹ Tel.: +1-404-651-4192.

tion gathered. Although privacy practices have improved over the last several years, 97% of websites collect personal information from visitors, yet only about half meet basic standards of privacy disclosures and fewer still—only 20%—meet Federal Trade Commission (FTC) standards for a comprehensive privacy policy (FTC, 2000).

For the “dot-coms,” practical considerations will undoubtedly influence attitudes toward privacy protection and the need for legislation. The relationship between privacy protection and marketing efficiency is complex because of the explicit tradeoff between information availability and consumer privacy concerns (Cook, 1995; Culnan and Armstrong, 1999). In a remarkably prescient article examining interactive marketing, Blattberg and Deighton (1991, p. 12) eloquently capture both the pros and cons of collecting marketing information.

There is a concern that personal information might be used in fraudulent schemes against naïve or unsuspecting people. More generally, there is a fear of the unfamiliar, information that strangers are not ‘supposed’ to know, used in ways that buyers never expected, gives an unfair advantage to sellers in adversarial marketplace relationships.

Privacy, however, comes at a price. Better market data makes marketing more efficient, and in competitive markets, the fruits of efficiency are passed on to consumers in the form of lower prices and greater choice. If the availability of better data lowers the cost of reaching a niche market, for example, then products that might never have been brought to market can be launched, and products that would have been expensive become affordable.

Moreover, when a company can more precisely target its prime customers, there is a reduction in the number of unwanted commercial intrusions as wasteful communication is reduced or eliminated (Blattberg and Deighton, 1991).

The ability of information brokers and marketers to collect, bundle and distribute information has been further enhanced by one of the major factors driving the growth of the Internet—the availability of increasingly inexpensive computing power. The data collected by marketers from government sources, other marketers, websites and even information furnished by consumers themselves when filling out warranty cards and other documentation is compiled into massive databases containing information on millions of Americans (Berry et al., 1994). Though this process produces marketing efficiencies (Blattberg and Deighton, 1991), it raises a different sort of dilemma for regulators and consumers. Information that is seemingly innocuous can be gathered and synthesized to produce a portrait that is accurate enough to make many consumers uncomfortable. The issue here is not necessarily the legitimate information that may be collected by marketers, but what can be done with this information when it is compiled.

At least one study indicates that consumers are not especially concerned about privacy compared to other issues

related to direct marketing (Milne and Gordon, 1993), and there is some indication that the largest commercial information collectors are the least likely to be abusive of consumer privacy (Boza and Milne, 1997). Anecdotal reports, however, suggest that privacy issues are important to consumers and that perceived privacy invasions by private companies, like those by governmental entities, can draw a nearly instantaneous and overwhelming public response.

A Harris-Westin telephone survey conducted during April 1997 polled 1000 computer-using adults regarding online privacy issues. Results indicated that 58% of the respondents favored having government “pass laws now for how personal information can be collected and used on the Internet” (Westin, 1999, p. 66). In a 1990 incident, Blockbuster Video announced that they were considering selling rental pattern information. The torrent of criticism they received in response to the announcement prompted them to drop the plan (and Blockbuster does not even rent x-rated titles) (Bloom et al., 1994; Miller, 1990). Similarly, in 1997, Lexis-Nexis discontinued their practice of including social security numbers with their “people search” feature due to an enormous public protest (Gilje, 1996). In a similar incident, the Federal Deposit Insurance (FDIC) abandoned plans requiring banks to monitor their customers’ accounts and report suspicious transactions to federal authorities. The “Know Your Customer” program drew so much criticism, partly in the form of “flaming” e-mail messages from bankers and customers, that the FDIC revised its plans (Day, 1999) and subsequently dropped the proposal entirely (FDIC, 1999; Tanoue, 1999).

Though these events suggest that privacy invasions can be countered by public protest, it is more common that privacy invasions go unnoticed by all except the most vigilant. Ninety-three percent of Americans believe that companies should be required to request permission before selling personal information about customers (Lacayo, 1991). But unless they are riled by some specific privacy invasion, Americans have not, until recently, shown much interest in stopping data collection and dissemination efforts by private companies.

In an effort to shed some light on the current state of privacy law in the United States and its relationship to e-commerce, this paper examines different regulatory mechanisms that protect privacy and their strengths and weaknesses. We review the regulatory status of data collection and dissemination in several categories of sensitive information: medical records, credit information, financial records, video rentals and cable viewing histories, school records, data collection from children, employment records and insurance information. Although this list is by no means exhaustive, these record categories represent some of the most sensitive privately held information. Such records, when bundled with social security identifiers and other publicly available information, have serious implications for informational privacy.

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات