PRIVACY AND SECURITY ISSUES IN E-COMMERCE

Privacy the control over one's personal data and security the attempted access to data by unauthorized others are two critical problems for both e-commerce consumers and sites alike.

Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both. This chapter reviews the current state of the art and the relevance for privacy and security respectively. We examine privacy from social psychological, organizational, technical, regulatory and economic perspectives. We then examine security from technical, social and organizational and economic perspectives.

Privacy

Privacy is a serious issue in electronic commerce, no matter what source one examines. Fisher [2001] reported "Forty-one percent of Web buyers surveyed last year by Forrester Research of Cambridge, Mass., said they have contacted a site to be taken off their databases because they felt that the organization used their information unwisely." A Business Week/Harris Poll found that over forty percent of online shoppers were very concerned over the use of personal information and 57% wanted some sort of laws regulating how personal information is collected and used [Harris Poll 2000]. Similarly, Culnan argued that privacy concerns were a critical reason why people do not go online and provide false information online.

Why this concern about privacy? The answer is simple. As of 1998, the FTC found that the majority of online businesses "had failed to adopt even the most fundamental elements of fair information practices. Indeed, relatively few consumers believe that they have very much control over how personal information, revealed online, is used or sold by businesses The combination of current business practices, consumer fears and media pressure has combined to make privacy a potent problem for electronic commerce.

Tackling privacy, however, is no easy matter. If nothing else, privacy discussions often turn heated very quickly. Some people consider privacy to be a fundamental right; others consider it to be a tradable commodity. Detailed arguments about the historical progression of privacy can be found, for example, in [Davies 1997] and [Etzioni 1999]. (Even these historical accounts have sharply differing viewpoints. For example Etzioni argues that privacy is societally illegitimate or infeasible, while Davies argues that it has become a squandered right.) For the purposes of this article, we will explore the potential space of privacy concerns, not privileging any particular viewpoint. In our view, both consumers and businesses may have legitimate viewpoints, sometimes conflicting. This is in the nature of most societal issues. We also restrict ourselves to the privacy issues that accrue in electronic commerce; we omit, for examples, the issues emerging from vehicle tracking chips, the wholesale monitoring of telephone and other communication mechanisms and image recognition from public cameras.

Scanned with CamSca

Social and business issues

Why is privacy of concern to e-commerce? We believe this concern stems from a new technical environment for consumers and businesses, the resulting data flow with substantial benefits to businesses and consumers, consumer concerns in this new environment and regulatory attempts to govern this environment. It is important to understand each one of these and to understand the tradeoffs. Privacy as a business issue is extremely sensitive to changes in the surrounding context. Changes in people's expectations (such as when they become accustomized to data transfer in commercial settings) or in regulatory governance (such as new laws, governmental regulations, or even case law in the US) can dramatically alter business issues and possibilities.

Below is an overview of the research and business issues. This will include the consumers concerns, technical issues and regulatory attempts to ameliorate privacy concerns. In this examination, our attempt is not to predict what will happen or should happen, but to present issues to guide further research and business activity.

Clearly, there are many business opportunities in the changing technical environment. The use of digital systems allows data capture at a much larger rate and scope than previously; e-commerce sites could potentially collect an immense amount of data about personal preferences, shopping patterns, patterns of information search and use and the like about consumers, especially if aggregated across sites. Not only is it easier than ever to collect the data, it is also much easier to search these data. New computational techniques allow data mining for buying patterns and other personal trends. These data can be used to personalize a customer's e-commerce experience, augment an organization's customer support, or improve a customer's specific e-site experience. The data are valuable for reuse, for example, in finding potential sales to existing customers. As well, the data are also valuable to aggregators (who may look for other personal trends and patterns) or for other types of resale. Indeed, reuse and resale are simultaneously both potential opportunities and problems. "Ironically, the same practices that provide value to organizations and their customers also raise privacy concerns".

Technologies for Privacy

The next consideration is technology. A number of technologies have altered the current privacy debates. There are technologies used for surveillance,the technologies for forming agreements (contracting) about the release of private data, the technologies for labeling and trust and privacy enhancing technologies (PETs).

The technologies for surveillance and for data capture are used by companies for business purposes, but they have the side effect of endangering personal privacy. These include generating data trails, data warehousing and data mining and biometrics. Many of these technical mechanisms can lead to consumer profiles that "are no longer based only on the individual's dealings with a single organization, because their data is shared by multiple merchants."

Balancing these tracking mechanisms are privacy enhancing technologies (PETs), which attempt to defeat or neutralize the surveillance or tracking technologies. Basic PETs include cookie-managers and personal firewalls. Other PETs attempt to provide genuine anonymity and include anonymous remailers (e.g., Mixmaster) and digital cash (*e.g.,* ECash). An active area of research and development are systems to provide non-traceable identifiers (*e.g.,* ZKS Freedom, AT&T Crowds, anonymizer.com, anonymous remailers). Yet other PETs, which Clarke calls "gentle PETs", try to balance privacy and accountability.

Scanned with CamSca