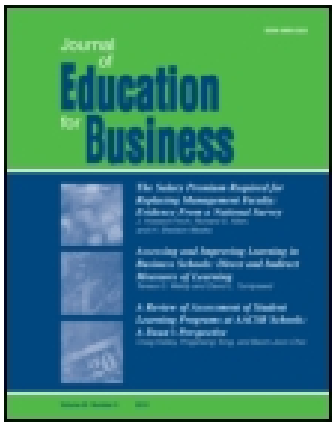
This article was downloaded by: [Aalto-yliopiston kirjasto]
On: 26 August 2014, At: 13:44
Publisher: Routledge
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Journal of Education for Business
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/vjeb20

E-Commerce and Privacy: Conflict and Opportunity

Badie N. Farah [a] & Mary A. Higby [b]
[a] Eastern Michigan University Ypsilanti , Michigan
[b] University of Detroit Mercy Detroit , Michigan
Published online: 31 Mar 2010.

To cite this article: Badie N. Farah & Mary A. Higby (2001) E-Commerce and Privacy: Conflict and Opportunity, Journal of Education for Business, 76:6, 303-307, DOI: 10.1080/08832320109599653

To link to this article: http://dx.doi.org/10.1080/08832320109599653

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at http://www.tandfonline.com/page/terms-and-conditions

E-Commerce and Privacy: Conflict and Opportunity

BADIE N. FARAH
Eastern Michigan University
Ypsilanti, Michigan

MARY A. HIGBY
University of Detroit Mercy
Detroit, Michigan

Downloaded by [Aalto-yliopiston kirjasto] at 13:44 26 August 2014

ABSTRACT. As e-commerce expands, Web sites increasingly collect, process, and sometimes divulge personal information about their customers without the customers' consent. In light of the limited success of several e-commerce initiatives to guard privacy, the Federal Trade Commission has recommended that Congress consider legislation similar to that existing in the European Union to guarantee customers' privacy online. The authors discuss the conflict between the e-commerce community's need to collect data and customers' desire to protect their privacy, the privacy tools available to deal with these issues, the possible impact of privacy laws on the future profitability of e-commerce firms, and privacy as a component of any course involving e-commerce.

Today, consumers go on the Internet to browse, learn about products, shop, and buy a variety of goods and services. Individuals with access to the World Wide Web approach the medium as a marketplace full of information. It is an increasingly convenient and easy environment in which products and services can be purchased and, in the case of digital software products, delivered. It also provides for maintaining a relationship with the customer for customer service and follow-up information on new products or services. The "commerce" in e-commerce encompasses all of these activities and more (U.S. Department of Commerce, 2000).

E-commerce is a technology-enabled application environment that facilitates an on-line, automated business transaction. This application can be implemented via a number of electronic means such as personal computers, digital personal assistants, and Web-enabled cellular phones. E-commerce transactions include microcommerce, e-tailing, and e-business.

Microcommerce refers to an e-commerce transaction with low value, such as the selling of a newspaper article for $.10 over the Internet. Microcommerce transactions are used rarely.

E-tailing is the same as retail sales, but with the Internet it is used as a transaction medium. This type of transaction includes a wide range of online consumer purchases of items including airline tickets, hotel rooms, and shares of stocks. The transactional component of this activity is the major focus of e-tailing. The most common type of e-commerce transactions are businesses-to-business, accounting for approximately 80% of all Internet sales transactions (Craig, 1998).

E-commerce transactions are only one way in which businesses can use the Internet to enhance their operations and increase their productivity. All businesses have information components that could be shared and communicated among employees and customers. E-business allows for the exchange of business information and the completion of business transactions. The following transactions are considered e-business: online marketing, EDI (electronic data exchange), and SCM (supply-chain management), just to name a few. Online marketing transactions are e-tailing transactions, whereas EDI and SCM are business-to-business transactions.

The Growth of E-Commerce

Since the inception of the Internet in the mid-1990s, e-commerce has grown at a very rapid rate. Current data indicate that as many as 90 million Americans use the Internet regularly (Federal Trade Commission, 2000). Of these, 96% shopped online in the third quarter of 1999. Fifty-four percent of Internet users have purchased products or services online. The Census Bureau estimates that retail e-commerce reached $5.3 billion in the fourth quarter of 1999, and other estimates place total e-tailing in the range of $20–$33 billion

for 1999. The latest data indicate that retail customers spent $2.8 billion online during January 2000 (Federal Trade Commission, 2000).

Because of such exponential growth in public interest and use of e-commerce, there has been a similar growth in online advertising revenue. Internet advertising expenditures climbed to $4.6 billion in 1999, representing a 141% increase over 1998 figures and a greater than 10-fold increase from 1996 (Federal Trade Commission, 2000).

Privacy Concerns

As Internet-related activities have exploded, so has data gathering by marketers tracking the consumers' online activities. This information is typically sold or disclosed to other entities or used to reach the consumers in electronic advertising campaigns. For example, consider the case of Amazon.com. This firm is on the forefront of the activity of collecting data and profiling its customers. Customers returning to their Web site are given a suggested list of books and videos based on their past purchase behavior. However, Amazon.com has not yet sold its customers' list or divulged their profiles to other entities and promises not to do so. Amazon.com shares customer information only with the subsidiaries it controls (Amazon.com, 2000).

In an analysis of data collected from Internet users, AT&T Labs (1999) found that

- Internet users are more likely to provide information when they are not identified.
- Users are more comfortable providing preference data than credit card numbers.
- Customers were concerned whether information was to be shared with other entities.
- Customers were concerned about persistent identifiers.
- Internet users do not want tools that transfer information automatically to Web sites.
- Users indicated that they would be more likely to provide personal information if there were privacy laws and policies in force.

It is clear from the previous discussion that marketers are openly violating the consumers' right to privacy and that consumers are worried about this trend. We believe that it is time for companies to take reasonable steps to protect consumers' privacy. However, because companies may not respect all aspects of consumer privacy, it is necessary for the government to step in and legislate the minimum requirements. In this article, we discuss tools that are currently available to protect consumers' privacy, examine the current business model used in e-commerce in the United States, and suggest possible ramifications or changes in privacy laws in the business model. In addition, we discuss the need to include a privacy component within an e-commerce course or any module on e-commerce in a business course.

Privacy Tools

Several tools exist for the protection of customers' privacy on the World Wide Web. These tools became available after widespread backlash from users of e-commerce Web sites. Customer privacy tools are being implemented on a voluntary basis at the present time. Among the most important tools used are TRUSTe, BBB*Online* Privacy Seal, and Privacy Preferences Project (P3P). A more recent tool, which has been advocated in the United States, is the privacy law. Some countries, including the European Union (EU), enforce privacy laws, whereas others such as the United States are working to legislate such laws.

E-Commerce Self-Regulation and Seal Programs

E-commerce self-regulation regarding consumer privacy has occurred through the development and implementation of seal programs. These programs mandate that their licensees implement certain fair information practices and submit to a variety of compliance monitoring orders in order to display a privacy seal on their Web sites (Internet Advertising Bureau, 1999, 1997).

TRUSTe was the first online privacy seal program (Federal Trade Commission, 2000). More than 1,200 Web sites have implemented this program in a variety of e-commerce businesses. Over 500 Web sites have been licensed to post the BBB*OnLine* Privacy Seal (The Council of Better Business Bureaus) since the program was launched in March 2000. The CPA WebTrust program, which includes a privacy component in its requirements, has licensed its seal to 28 Web sites; and six companies have been licensed to post PriceWaterhouseCooper's BetterWeb online privacy seal (Federal Trade Commission, 2000).

Privacy Preferences Project

Privacy Preferences Project (P3P) refers to a new technology standard comprising a set of computer-language protocols that let on-line consumers set their own levels of privacy when browsing the World Wide Web (Federal Trade Commission, 2000). The basic assumption behind these protocols is that they prevent the consumer from inadvertent transmission of personal data. Web site privacy policies include a wide range of practical details. The P3P specifications include protocols for encoding these practices in a standard fashion. However, it is unclear how to best (a) display these practices in a way that the user can evaluate the practices quickly and (b) design a user interface that permits the user to configure an automated tool for evaluating those practices (AT&T Labs, 1999).

P3P is software that tells an online user what kind of personal information a Web site collects about a visitor. The customer tells the P3P software which personal information he or she will release. The e-commerce site alerts the customer if it wants more information and what it will do with the information if provided. The major concern is what the site will do if the customer refuses to provide the requested information. Should the site be allowed to deny the customer entry if such information is not furnished?

The World Wide Web Consortium developed the P3P technology. The Massachusetts Institute of Technology and universities in France and Japan operate this Consortium. The P3P pro-

Downloaded by [Aalto-yliopiston kirjasto] at 13:44 26 August 2014

ject is likely to become a standard because the World Wide Web Consortium is supported widely by the computer and Internet industries. Microsoft Corporation plans to install P3P in the next version of its Windows operating system. Further, the Clinton administration said that it supported this standard, and the White House incorporated the P3P standard into its Web page. Any browser with P3P software will be able to interpret the White House Web pages' privacy policies.

P3P requires the customer to "opt out" in order to protect his or her privacy. Privacy activists say the customer will never bother to opt out, because P3P requires an unreasonable amount of initiative on the part of the consumers to protect their privacy.

Privacy and Legislation

Three important questions need to be answered in the privacy debate:

1. Should e-commerce users have to "opt-out" by informing companies that they do not want their personal information sold or given to marketers or any interested party?
2. Should e-commerce companies have to ask users' permission first, requiring users to "opt in" to a consent agreement that frees their personal information for use in the public domain?
3. Should the current system under which e-commerce companies buy, sell, or share personal information in an unrestricted manner stay intact?

The U.S. Congress is considering a large number of legislative options to address the concept of on-line privacy. The proposed laws could increase the rights of e-commerce users dramatically with respect to the personal information they provide the Web sites as they surf through cyberspace.

Another proposal advocates the use of a privacy "czar" to coordinate information sharing among federal agencies. Many of those agencies have chief information officers responsible for privacy issues among other duties (Associated Press, 2000).

The difference between the U.S approach to online privacy and that of the European Union is rather pronounced. The United States has relied mainly on market forces, counting on the customer to reject unduly probing Web sites. On the other hand, the European countries have established privacy laws for e-commerce, and the Web sites must adhere to stringent guidelines. The European Parliament enacted guidelines, titled the "European Community Directive on Data Protection," that require member states to enact laws for the protection of personal information. In addition, the directive prohibits member states from transmitting personal data to countries that do not have privacy laws to guarantee the protection of personal information. The United States does not have such privacy laws.

For Europeans surfing U.S. Web sites, the United States and the European Union have reached a compromise on privacy issues called the "safe harbor" agreement (EU Working Group of Privacy Commissioners, 1999), a set of privacy guidelines that the U.S. Web sites can follow to gain a "safe harbor" from EU legal ramifications. However, compliance is voluntary because it is not clear what EU officials can or will do about any violations.

The safe harbor agreement requires that Web sites collecting personal data must tell visitors which data is being collected, for what purpose, and with whom it will be shared. Further, the agreement stipulates that customers have the right to view their personal data and, if necessary, correct any misinformation (EU Working Group of Privacy Commissioners, 1999). Both the European governments and American privacy advocates believe that the safe harbor accord cannot be enforced because of what they perceive as U.S. companies' poor record with self-policing privacy policies.

The Federal Trade Commission recommended that Congress adopt legislation that provides a basic level of protection for consumers in an e-commerce environment. The legislation would establish basic standards for the collection and use of data on-line and provide an implementing agency with the authority to promulgate more detailed standards. E-commerce sites that collect personal information from or about consumers online would be required to adhere to the four accepted fair information practices of notice, choice, access, and security.

Notice

E-commerce Web sites would be required to provide customers with clear and conspicuous notice of their intent to collect data directly or indirectly; how they would use that data; how they provide customers with choice, access, and security; whether they would provide that data to other entities; and whether other entities would be allowed to collect data from the site.

Choice

E-commerce Web sites would be required to offer customers choices about the use of their personal information beyond what is necessary to complete a transaction. The choices apply to secondary uses by the same Web site (such as marketing back to the same customer) and to external uses (such as selling or providing the data to other entities).

Access

E-commerce Web sites would be required to provide customers access to the personal information collected about them. Further, customers should be able to review, correct, or delete such information.

Security

E-commerce Web sites would be responsible for taking reasonable steps to keep the customer data that they collect secure (Federal Trade Commission, 2000).

Impact on the Business Model

E-commerce firms have always kept information on consumers' habits to target people for specific products. Customers provide their names, addresses, credit card numbers, and phone numbers to e-commerce Web sites when placing orders. Further, some Web sites require customers to register before

Downloaded by [Aalto-yliopiston kirjasto] at 13:44 26 August 2014

granting them access to the site; thus these customers offer their personal information voluntarily. Sometimes customers divulge extensive personal information to get free merchandise or enter a drawing for prizes. Consumers who browse e-commerce sites have their habits tracked by means of electronic files called "cookies." These files are transferred from certain Web sites to the consumer's computer while the user is online. The cookies map the behavior of the customer, allowing e-commerce sites to create an online profile of his or her interest in browsing and purchasing. E-commerce sites often deny access to customers who disable cookies on their personal computers.

The use of cookies allows e-commerce sites to tap vast amounts of personal data useful in their pursuit of efficient and effective marketing to individuals who have visited specific sites. Many industry leaders have suggested that such cookies are in part the reason why the Internet remains free of charge. Such large amounts of detailed personal information provide a rich source of income for most e-commerce companies.

Privacy laws, if enacted, most likely would require that e-commerce customers "opt in" before a Web site can collect any personal data. This requirement could add a considerable cost to the e-commerce operation because customers are less likely to opt in than they are to opt out when given the opportunity to forbid the sharing of data. The loss of data would be a blow to e-commerce businesses' efforts to establish large databases of marketing information. Those businesses would face higher marketing costs as they try to compensate for the data loss through less-efficient methods of targeting potential customers.

In addition, when privacy regulations are applied to e-commerce, strict auditing of business compliance will add to the cost of operations. The economic impact of privacy laws on e-commerce businesses has not received enough scrutiny from regulators and probably will not be evaluated fully until after such laws are passed.

Customer data is a gold mine for e-commerce companies. If companies are limited in collecting and mining data via regulation, their profits will erode. Such regulation will lead to the need to change the existing free-of-charge business model. A different business model that complies with restricted privacy laws might be manageable by e-commerce companies but may reduce their profitability.

The e-commerce industry, meanwhile, is working very hard and hoping to convince the regulators (the Federal Trade Commission and Commerce Department) to let them draw up a set of voluntary rules that would place new, and more stringent, restraints on online consumer profiling. Under these voluntary rules, online marketers would provide customers with better notice on use of data, as well as clearer explanations of privacy policies. These voluntary rules might forestall restrictive legislation until new technologies are developed. One such technology is the development of software that anonymously provides the same customer profile for online marketers without keeping a record of the customer's behavior. For example, a customer's surfing record could be manipulated by software to produce an "electronic silhouette" of the customer, after which the surfing record (the click-stream data) is destroyed, leaving no track of the customer's behavior or identity anywhere. The electronic silhouette would provide all the important information for marketers, thus preserving their ability to collect data and profit from it, and at the same time preserve customers' privacy.

Several business models that are not dependent on profiling customers for free may be developed. A possible business model would involve a customer's paying a small fee for allowing an e-commerce firm to record his surfing data stream for the purpose of profiling his behavior. The e-commerce firm would use such profiles to market to customers and/or sell these profiles to other firms for marketing purposes. Specifically, the customer would be selling his or her personal information to the e-commerce firm, and the firm would use it for marketing.

However, too much restriction may cause the business model to change to one that charges the user a small fee to make up for lost revenue. Another possible business model could involve providing customers with a choice of access arrangements, ranging from full and elaborate service for a fee to a very limited service without any fee. A customer may be charged per item. For example, an e-commerce Web site that helps a customer locate the auto dealer with the lowest price for a particular car model could charge the customer for each session during which it makes its data bases and expertise available to the customer. This scenario would also apply to cases in which the customer uses the e-commerce site to develop a personal financial plan. In the presence of restrictive privacy policies, it is likely that a high-quality free service will become a thing of the past.

Privacy in Business Education

Because e-commerce is included in virtually every business discipline from accounting, finance, management, and marketing to information systems, the components of any e-commerce course or topic must include a discussion of online privacy policy. As the potential enactment of on-line privacy legislation in the United States looms near, it becomes even more essential that the ramifications of e-commerce privacy be included within such discussions. As many firms have little value other than their customers' lists, it is essential that students understand that the success of many e-commerce firms in the future will depend greatly on the firms' adoption of viable privacy policies. For students to understand privacy polices adequately, they must not only be discussed as a topic of e-commerce but also covered in other activities. Case studies can be beneficial in allowing students to review, critique, compare, and contrast the policies of multiple firms to understand fully the ramifications of privacy for e-commerce firms. Furthermore, a case study exposing students to designing a privacy policy for an e-commerce firm would be very instructive.

Summary and Conclusion

Both voluntary privacy policies and legislative initiatives are necessary to

Downloaded by [Aalto-yliopiston kirjasto] at 13:44 26 August 2014

provide the protection of privacy of e-commerce customers. In this way, the e-commerce community can continue to evolve free of harsh and restrictive laws and regulations. However, certain laws must exist to reign in rogue businesses when they stray from acceptable practices. In addition, this combination of laws and voluntary policies will allow the laws to evolve with the technology rather than becoming a stumbling block. If the e-commerce community places certain restrictions on its own behavior, these restrictions in turn will help the laws evolve with the technology to cement the protection of the online customer. The e-commerce business community should be active in pursuing a compromise with the U.S. government—the Federal Trade Commission, the Commerce Department, the White House, and/or the Congress. Such a compromise will satisfy the needs of both the e-business community and its customer within a manageable time frame that allows the technology to catch up with the needs of society. In addition, an e-commerce community active in drafting a compromise rather than reacting to a law would reduce the damage to the current business model and allow a variety of business models to develop.

As e-commerce applications explode, students must have an understanding of privacy policies and their impact on e-commerce. Because so many functional areas of business are concerned with e-commerce, a privacy component is mandatory in any course for students to understand the implications, development, and implementation of such policies. This article can serve as a concise resource for business students in the area of privacy in e-commerce.

REFERENCES

Amazon.com. (2000, September 4). *Amazon.com Privacy Notice* [On-line]. Available: http://www.amazon.com/exe/obidos/subst/misc/policy/privacy.html/

Associated Press. (2000, August 21). Some in Congress say U.S. Government could use an Information-Privacy Czar. *The Wall Street Journal* [print], B6.

AT&T Labs. (1999, April). Research Technical Report TR 99.4.3. *Beyond concern: Understanding Net users' attitudes about online privacy* [On-line]. Available: http://www.research.att.com/library/trs/99/99.4/

Craig, A. (1998, August 28). Streamlining business drives e-commerce. *Internet Week Online* [On-line]. Available: http://www.planetit.com/

EU Working Group of Privacy Commissioners. (1999). *Safe Harbor Draft Agreement.* [On-line]. Available: http://europa.eu.int/comm/internal_market/en/media/dataport/index.htm

Federal Trade Commission. (2000, May). *Privacy online: Fair information practices in the electronic marketplace.* A Report to Congress [On-line]. Available: http://www.ftc.gov/reports/privacy3/index.htm

Internet Advertising Bureau. (1999). *Internet Advertising Bureau announces 1998 Advertising Revenue Reporting Program results* [On-line]. Available: http://www.iab.net

Internet Advertising Bureau. (1997, March 25). *Internet Advertising Bureau announces 1996 Advertising Revenue Reporting Program results* [On-line]. Available: http://www.iab.net

U.S. Department of Commerce. (2000, June). *Digital economy 2000.* Economics and Statistic Administration Office of Policy Development [On-line]. Available: http://www.ecommerce.gov

Downloaded by [Aalto-yliopiston kirjasto] at 13:44 26 August 2014