Are E-Privacy and E-Commerce a Contradiction in Terms? - An Economic Examination

Dirk Frosch-Wilke
University of Applied Sciences, Kiel, Germany
dirk.frosch-wilke@fh-kiel.de

Abstract

At first glance, electronic commerce seems to be inconsistent with electronic privacy. Personalization plays an important strategic role in e-commerce. Thus, a lot of information about online consumers are collected, analysed and used. By contrast, e-privacy is aimed at reducing the amount of collected information about the Internet users. On the other hand recent empirical studies show that lack of confidence in privacy protection of e-commerce environments results in lower sales in the business-to-consumer segment. The key contributions of this paper are to elaborate on general relations between e-commerce and e-privacy from an microeconomic perspective, to identify economic consequences entailed by lack of privacy protection, and to identify economic reasons for increasing personalization in e-commerce.

Keywords: Internet, electronic commerce, privacy, user control functions, economic analysis of privacy protection

Introduction

It seems that for profitable electronic commerce online collection of vast amounts of user data is inevitable. Activities as data mining, one-to-one marketing, customer-relationship-management (CRM) etc. are very popular instruments of organizations in the growing business-to-consumer market. All these activities require a lot of – also sensitive - data of customers. Simultaneously technologies (e.g. http protocol, cookies, web bugs, global unique identifier) and computerized databases make automated collection and processing of information particularly easy and convenient for an Internet company. The individual is often not aware of the data trail it leaves behind when using the Internet. Furthermore, many business models of online advertisers intend to monitor the behaviour of users on the Internet and to provide online profiles of them. Meanwhile personal data of Internet users are an important commodity (Berman, 1999).

On the other hand, concerns of Internet users about online privacy grow (Pitofsky, 2000b) and governments of many countries – above all of European countries - are confronted with a manifold dilemma:

- Legislative actions for privacy protection only refer to territorial borders and therefore have limited effect in a global network.
- Governments do not want to weaken the economic prosperity developing in many countries not to the least on the ground of prosperity of the Internet economy, and therefore they refrain from constraining national regulations.
- Legislative measures can hardly match with the needs of the fast Internet development because of the protracted process of legislation.

In response to buyers' concerns about privacy, some companies – above all US-companies -take part on privacy seals programmes. Even this self-regulation approach does not seem an appropriate way to protect the privacy interests of Internet users. That's why the US Government has started initiatives aimed at helping to improve online privacy protection.

In summary, we can observe a lot of uncertainties on the online business-to-consumer markets about privacy for all three interest groups: Buyers, governments and also sellers.

For this reason we will have to consider the relation of privacy and commerce on the Internet with care, mainly from an economic and less from a legal and technical perspective. Based on recent empirical studies we will show that transparency in collection, use and dissemination of customer data as well as enabling users to influence this process, are critical prerequisites for success of Web com-

panies. Nevertheless, economic analysis of privacy protection is still missing in the science of business management.

The contribution of this paper is that it focuses privacy protection in electronic commerce markets from a general economic perspective. Other papers about Internet privacy mainly stress legal technical or organizational aspects (e.g. Bermann, 1999, Cranor, 2000, van Gigch, 2000). On the other hand, microeconomic analysis of e-privacy is still missing. In Hoeren's paper (Hoeren, 2000) mainly the costs of regulation have been investigated. We will additionally stress costs of self-regulation programmes and much more important substantial economic consequences of privacy protection especially on returns and on costs of Internet companies. This paper cannot be an extensive economic analysis of online privacy protection but it intends to be a first step towards it.

E-Privacy and E-Commerce – a Description of State

For most organizations worldwide „digital business" is a tremendous challenge. To mention only a few implications of spreading digital business technologies: new technologies make spatial and temporal limitation obsolete, classical barriers for market entry have less significance in a world of virtual shops, the Internet enables information transparency, and customers demands on service quality are growing.

A growing number of companies accept these challenges and understand digital business technologies as a chance to increase corporate performance and to gain substantial advantage over competitors. Speed and customer-focused responsiveness are the watchwords (Vervest, 2000, p. 21).

Customer-focusing and access to actual information about the individual customer at any time are important elements of corporate e-commerce strategy. It is not surprising that e-commerce consultants recommend the collection of a multitude of information about Internet users: "...persuade users to provide personal information and preferences, and also[...]track the electronic trail they leave as they make active choices,[allow] infomediaries to gather information of great value to advertisers and to suppliers..." (Vervest, 2000, p. 67).

There are many technologies and business models to accumulate (anonymous) information about Internet users or to get personal customer information. Few examples are:

- Offering free services if the consumer will fill in an extensive questionnaire,
- Use of cookies or web bugs which are able to track Internet users activity at a particular Web site or from Web site to Web site such that users do not become aware (Wiese, 2000).
- Logging of incoming requests to an access log file.

Meanwhile use profiling is an important element in business practices of network advertisers, like DoubleClick or Be Free. They are able to monitor the behaviour of users in the Internet with cookies and webbugs because they have placed advertisements on thousands of Web sites (e.g. DoubleClick has webbugs on more than 51,000 web sites in September 2000 (Smith, 2000)). Every time a user will visit a Web site equipped with an advertisement banner placed by a network advertising firm, these network advertiser can make use of cookies and webbugs.

Use profiles are employed by network advertisers for targeted fade-in of banner ads. Employment of use profiles could be more effective if they are associated with personally identifiable information (e.g. name, age, profession, address) becoming „personal profiles" (for personal profiling see (Larsen, 1992)).

In July 2000 DoubleClick failed with the attempt to match anonymous use profiles of Internet users with information of the Abacus database which contains names, addresses and retail purchasing habits of 90% of US-American households, after "...privacy advocates lambasted DoubleClick for its actions and several governmental bodies launched investigations of the company's business practices." (Rodger, 2000b)

Not only privacy advocates and public authorities worry about privacy on the Internet, but also the Internet users:

- A May/June 2000 survey of Pew Internet found that 84 percent of US net users are concerned that companies are able to get personal information about themselves and their families (Fox, 2000).
- An October 1999 survey by IBM found that 72 percent of net users are worried about Internet privacy. The study also found that only 21 percent of consumers trust Internet companies, and that 57 percent of Internet users in the USA (41 percent in UK, 56 percent in Germany) decided at some point not to purchase a product online because of privacy concerns (Sever, 1999).

Internet users are not in majority against providing personal information, but they want to decide about the collection, use and dissemination of their personal data (so called

"opt-in" user option) as the Pew Internet survey of May/June 2000 found:

- 64 percent of US net users would transmit personal information in order to use a Web site and
- 86 percent are in favour of "opt-in" privacy policies that require Internet companies to ask people for permission to use personal information.

Most corporate privacy policies are inconsistent with this user demand for „opt-in" policies. Certainly there exist some self-regulatory activities of Internet companies, such as disclosure of privacy notices on their Web sites or joining online privacy seal programs, like TRUSTe or BBBOnlinePrivacy. A May 2000 study by the Federal Trade Commission found that 8 percent of all US commercial Web sites and 45 percent of the 100 busiest Web sites have a privacy seal (Pitofsky, 2000a). The study also found that of the commercial sites with a privacy seal 52 percent (56 percent of the busiest sites with a privacy seal) have, at least in part, all four of the fair information practice principles of Notice, Choice, Access and Security implemented (Pitofsky, 2000b).

This means that only 4 percent of all commercial US Web sites have implemented „opt-in" privacy policies. Furthermore, the question of enforcement, i.e. the use of effective sanctions in the case of non-compliance, is still open for these self-regulatory programs.

On the other hand also in states of the European Union (EU) which follow some regulatory approach in privacy protection (see e.g. EU Directive 95/46 (EU, 1995)), effective sanctions are missing in the privacy laws, or privacy protection authorities have not the necessary qualifications or not enough capacities (Schaar, 2000). Governments strive for regulations of frontier crossing data flows, e.g. the EU and the USA with the „Safe Harbor Principles" agreement in response to the above mentioned European Commission Directive on Data Protection that could interrupt transfers of personal information from Europe to countries whose privacy practices are not deemed "adequate" (see e.g. (Dix, 2000)). However, the problem of an effective enforcement and existence of trustworthy instances is still unsolved and the Safe Harbor agreement does not enforce opt-in regulations.

From a more technical point of view the World Wide Web Consortium (W3C) is engaged in privacy protection in the Internet. Since 1997 the W3C develops the „Platform for Privacy Preferences" (P3P). The goal of P3P is to enable users to exercise preferences over Web sites' privacy practices. But the actual P3P specification (Version 1.0) builds only two of the four fair information practices, that is notice and choice (Grimm, 2000). Nevertheless P3P will enable the Internet users to collect information of privacy policies of competing enterprises, to compare these policies and to choose those company whose policies correspond best with their own privacy preferences. P3P may enhance further e-privacy promulgation provided it is adopted by a critical mass of Web sites, if this will be achieved remains to be seen (Catlett, 1999).

In summary, electronic privacy protection attracts more and more attention of consumers and companies in electronic commerce. On both sides exist many uncertainties that reduce the growth and profitability of electronic commerce:

- Consumers mainly do not trust Internet companies and are worried about privacy protection for Internet communication. Therefore Internet users sometimes decide not to order online because they are not convinced that their personal data are treated confidentially, or they give misrepresentation of personal data at some point of a business transaction with a Web company because the meaning of the data collection is not transparent to them (Fox, 2000, p. 10).
- Consumers do not refuse to transmit personal data as a matter of principle because they also perceive the advantages of stronger customer-focusing which is not feasible without collection and use of personally identifiable information. They demand opt-in privacy policies, however.
- Internet companies response to public concerns by disclosure of privacy policies and joining privacy seals programs is unsatisfactory.
- Privacy protection laws often lack effective enforcement and protracted legislation cannot follow the fast progress of the Internet development.
- Technical solutions, as P3P, are able to make privacy policies of Internet companies more transparent and comparable but they cannot set up a privacy protection standard in the Internet. Perhaps P3P is unlikely to be ever adopted at an effective degree.

A Microeconomic View of Electronic Privacy

An economic analysis of privacy protection is still missing in the science of business management. Also in this paper we cannot develop such an analysis but we will show the possible benefits of a detailed economic estimation of online privacy protection activities within the scope of electronic commerce.

We will therefore discuss the conditions of privacy protection investments for achieving returns, the economic consequences of missing privacy protection and the possible economic benefits of an intensive collection and use of customer data. Concerning the costs of data protection we will differentiate between governmental privacy protection regulation and self-regulation efforts following different approaches in Europe and in the USA.

In what follows we will discuss three aspects:

- General economic consequences of online privacy protection
- Cost of governmental privacy protection regulation
- Cost of self-regulated privacy protection

General economic consequences of online privacy protection

Lack of measures for privacy protection, inscrutability in collecting and using customers data or abuse of customer data could have following negative consequences for costs and turnovers of Internet companies:

- *Not realized returns*: For many Internet users lack of trust in responsible usage of customer data by Internet companies contribute to avoid ordering online. In this case, the company cannot realize potential possible returns. Especially for many companies in the e-economy this is relevant because they have low variable costs and high gross margins per customer order. The reason for this is that these companies have often high levels of fixed costs (e.g. by strong investments in hard- and software and marketing activities) and low marginal costs per customer order because of the scaleability of information technology systems (e.g. marginal costs for information commodities are zero (Shapiro, 1999)). Thus, not realized customer orders have often more significant impact on Internet firms‘ profit-and-loss-account than to companies in the old economy.
- *Damage of companies‘ image*: Abuse of customer data, be it factual unlawfully or in public perception only, can significantly damage companies image. This means turnover losses because of customer migration. For Internet companies a damaged image often becomes an obstacle for the acquisition of new customers. On fast growing markets, as many markets in the business-consumer-segment of electronic commerce, customer acquisition has higher significance than on traditional markets (Rosemann, 1999). Therefore, Internet companies have to compensate for the damaged image through high marketing and public relation investments, resulting in higher costs per new customer acquisition.
- *Low stock market value*: The abuse of personal data could result in a lower stock market value, as the DoubleClick example shows: After the Federal Trade Commission confirmed an inquiry in February 2000, DoubleClick stock dropped 15.27% (Rodger, 2000a). A long-term low stock value will result in higher financing costs for the Internet company, because investors will demand higher profits of capital stocks and issues of new stocks will only be possible to lower prices.
- *Lower quality of market research results:* Missing trust in online privacy protection tempt Internet users to make false statements regarding their personal data. Therefore customer databases of Internet companies are sometimes full of faulty or incomplete data. Using these databases for market- and customer segmentation, as it is intensively done in connection with customer relationship management (Rosemann, 1999), end up in low quality segmentation approaches and therefore resulting in wrong or bad decisions about company activities.

In contrast we can identify following positive basic consequences of privacy protection:

- *Comparative competition profit*: As shown above, Internet users demand for „opt-in“ privacy policies. An Internet company can have an advantage over its competitors if it offers the opt-in option to its customers and is therefore able to satisfy customer needs better than the competitors (see e.g. (Porter, 1997, p. 153) for a more general view at the relation between customer preferences and competitive profits). This is much more relevant in electronic markets than in traditional markets as customers are able to find an alternative Internet company, which satisfies their needs better, with low transaction costs.
- *Higher customer retention rates:* Customers confidence in the company is a necessary condition for their loyalty. This is truer than ever on the Web, where business is conducted at distance and uncertainties are bigger because of impersonality in business relations (Reichheld, 2000). Informing users about privacy policy and to offer them the opportunity for opt-in are fundamental requirements for users‘ trust and thus higher customer retention rates.
- *More returns per customer:* “If customers do trust an online vendor, they are much more likely to share personal information.“ (Reichheld, 2000, p. 107) The effective use of this customer information allows Internet companies to offer customized products and services

(e.g. proactive service offerings) tailored to customers' individual preferences, which could generate higher returns.

Coming back to the last point, we will now discuss why the general use of personal customer information is exaggerated in e-commerce, though also in traditional markets many companies are about to implement an efficient customer relationship management (CRM). Thus information systems are used to learn more about their customers with the aim to maximize the influenced differences between returns and costs during the customer life-cycle (Rosemann, 1999).

Successful companies in e-commerce, like Amazon, Dell or AOL, use intensively customer information that enables them to build up close relationships with their customers. Reasons for this are:

- *Easier to get information about customers:* Customers in shops leave no record of their behaviour unless they buy something – and even then data are often not collected or , if retrieved, are sketchy. In virtual shops customers have to give up anonymity because products must be delivered to them or because anonymous payment methods, like digital cash, are not accepted. In some marketplaces of e-commerce (e.g. marketplaces using auctions as bargaining model) Internet users have to give up anonymity just before participating.
- *High outlays for acquiring customers*: Especially Web companies often have outlays to acquire customers that are considerably higher than for companies in the old economy. Pure-play Internet retailers, for example, have 20% to 40% higher new customer costs than traditional retailers (Reichheld, 2000). For many start-up Web companies with sometimes complete new business models it is necessary to acquire many customers just after starting business because they must fear competitors quickly entry into this new market. Other Internet companies, especially portals or navigation companies (see Evans, 1999), try to acquire high market shares because they expect a market consolidation in the next future where only companies with high market shares will survive. Therefore marketing and sales investments of these companies are sometimes higher than their turnovers, as the Lycos Europe example shows. (Lycos Europe N.V. turnover in the fourth quartal period of the business year 1999/2000 was 15.7 Mio. Euro whereas the sales and marketing costs were 56 Mio. Euro (Lycos, 2000).) Thus, Web companies have to achieve their full sales potentials with each customer to recoup their initial acquisition investments. As a result, they try to gather much knowledge about their customers and to use it for selling more products and services, e.g. through cross-selling.
- *Strengthening customer loyalty*: Web companies can use information about customers to form a more intimate relationship with them, offering customized products and services, which in turn strengthens customer loyalty (Reichheld, 2000). Since in most Web businesses the break-even for customer profit is two to three years, building long-term relationships is an important strategy of successful Internet companies.

After this general discussion about economic consequences of the use of information about Internet users, we now analyse costs of privacy protection. By doing this, we will not examine *implementation costs* more closely, i.e. costs for implementing the privacy protection norms of self-regulation or governmental regulation (e.g. investments in security technologies or software solutions like P3P). Nevertheless, a full economic analysis of e-privacy will have to include implementation costs.

Cost of governmental privacy protection regulation

Hoeren (Hoeren, 2000) distinguishes three kinds of regulated privacy protection costs:

- *Definition costs*: These are costs for the establishment of national privacy protection norms. On one hand, these costs are indirectly financed through companies taxes. On the other hand, definition costs include expenses for lobbyists, like business interest associations, which are financed through membership fees.
- *Monitoring costs*: These are expenses for controlling the compliance with privacy protection norms. In case of governmental monitoring these costs are indirectly financed through taxes and directly financed in case of self-monitoring.
- *Enforcement costs*: These are costs that are consequences of norm violations, like damages, contractual penalties or costs on account of contract nullification.

Quantification of these costs depends, especially for monitoring and enforcement costs, on the contents of national privacy protection laws (Hoeren, 2000). This concerns the amount of governmental norms as well as the responsibility for monitoring. For example, in Germany monitoring costs are high for organizations, because the German data protection law (BDSG, 1990) stipulates, that many companies have to nominate and to pay a data protection commissioner (BDSG §36). In this case monitoring costs are completely shift on to the companies.

Enforcement costs could be higher for a company, if competitors have the possibility of monitoring the compliance of data protection norms, because some data protection regulations are judged by their detrimental effects on competition, and therefore non-compliance of data protection norms could also be a non-compliance with competition protection norms.

Cost of self-regulated privacy protection

Using the classification of costs from above, we will demonstrate costs of self-regulation by means of an example. For this, we choose the privacy seal programme TRUSTe (http://www.truste.com).

- *Definition costs*: Costs for the licensee arise from definition of „privacy statements“, from the explanation of the corporate privacy and security practices to the licenser, from the support of the certification and review process through the licenser and from the licence fee.
- *Monitoring costs*: These are indirect costs because they are included in the licence fee. In privacy seal programmes the licenser is responsible for monitoring the privacy practices of the licensee. For this reason, the licenser encourage Internet users to announce to him license violations.
- *Enforcement costs*: In the USA non-compliance of published privacy policies could entail civil action against the company. Otherwise only in case of non-compliance with national data protection norms enforcement costs could arise. TRUSTe's only sanction is withdrawal of the privacy seal in such case, which may have extremely negative consequences for the licensee's image with the above discussed economic results.

Conclusion

In this paper, we have studied the business-consumer segment of electronic commerce seen from the view of privacy protection of Internet users. Recent empirical studies and concrete examples show that e-privacy is important for successful e-commerce.

Internet users are increasingly concerned about of technical and organizational corporate possibilities to collect and use sensitive user data. This development results in lower growth rate of online retailers‘ sales. Consumers use the Internet intensively for information purposes, but often they refrain from purchasing products or services online because they do not trust the way online companies will use their personal data.

Thus, for Internet companies it becomes strategically important to analyse the impact of building trustworthy e-commerce environments on their costs and returns. We have presented a first approach for a microeconomic analysis of privacy protection. In summary, we have shown that electronic privacy does not contradict electronic commerce a priori. We expect that companies, which makes their privacy policies transparent for Internet users and implement user control functions in their information systems for user's consent in collection personal data, revocation of this consent and inspection and removing of stored personal data (in (Enzmann, 2000) a prototype implementation of user control functions is demonstrated), could gain competition profits.

Further research in this area is indicated to focus some of the above-mentioned topics, to treat it at a greater microeconomic depth and to show consequences for the implementation and use of information systems.

References

Bermann, J., & Mulligan, D. (1999). Privacy in the Digital Age: Work in Progress. *Nova Law Review*, 23(2).

BDSG (1990). Bundesdatenschutzgesetz vom 20.12.1990 (German Data Protection Law).

Catlett, J. (1999). Technical Standards and Privacy – P3P. Accessed September 26, 2000 at http://www.junkbusters.com/standards.html

Cranor, L.F. (1998, June/July). Internet Privacy: A Public Concern. *netWorker: The Craft of Network Computing*, 2, 13-18.

Dix, A. (2000). Internationale Aspekte (International Aspects). In Bäumler, H. (Eds.). *E-Privacy*. Braunschweig, Wiesbaden:Vieweg, 93-106.

Enzmann, M., Pagnia, H., & Grimm, R. (2000). Das Teledienstdatenschutzgesetz und seine Umsetzung in die Praxis (The German Teleservices Data Protection Act and its Realization). *Wirtschaftsinformatik*, 42 (5), 402-412.

EU (1995). EU Directive 95/46 on dataprotection.

Evans, P., & Wurster, T.S. (1999). *Blown to Bits: How the New Economics of Information Transform Strategy*. Boston: Harvard Business School Press.

Fox, S. et al. (2000). Trust and privacy online: Why Americans want to rewrite the rules. Accessed August 25, 2000 at: http://www.pewinternet.org/reports/toc.asp?Report=19

Grimm, R., & Rossnagel, A. (2000): Can P3P help to protect privacy worldwide ?. *Proceedings of ACM Multimedia 2000 Workshops*, Oct 30-Nov 3, Los Angeles, USA, 157-160.

Hoeren, T. (2000): Datenschutz als Wettbewerbsvorteil (Privacy Protection as a Competitive Profit). In Bäumler, H. (Eds.). *E-Privacy*. Braunschweig, Wiesbaden:Vieweg, 263-279.

Larsen, E. (1992). *The Naked Consumer: How Our Private Lives Become Public Commodities*. New York: Holt & Co., 1992.

Lycos Europe N.V. (2000). Lycos Finance News from 09/05/. Accessed September 13, 2000 at http://pressroom.lycos.de/english/common/newsitem.asp?id=64

Pitofsky, R. et al. (2000a). Privacy Online: A Report to Congress. Federal Trade Commission. Accessed August 25, 2000 at http://www.ftc.gov/reports/privacy3/toc.htm

Pitofsky, R. et al. (2000b). Privacy Online: Fair Information Practices in the Electronic Marketplace – A FTC-Federal Trade Commission Report to Congress. Accessed August 25, 2000 at http://www.ftc.gov/os/2000/05/index.htm#22

Porter, M. (1997). *Wettbewerbsstrategie (Competitive Strategy)*. Frankfurt a.M.: Campus.

Reichheld, F.F., & Schefter, P. (2000, July-August). E-Loyalty: Your Secret Weapon on the Web. *Harvard Business Review*, 105-113.

Rodger, W., & Farrell, G. (2000a). Investors dump DoubleClick. *USA Today*, 02/17/2000. Accessed August 25, 2000 at http://www.usatoday.com/life/cyber/invest/in386.htm

Rodger, W. (2000b). DoubleClick backs off Web-tracking plan. *USA Today*, 06/07/2000. Accessed September 6, 2000 at http://www.usatoday.com/life/cyber/tech/cth486.htm

Rosemann, M., Rochefort, M., & Behnck, W. (1999). Customer Relationship Management (in German). *HMD-Praxis der Wirtschaftsinformatik*, 36(208), 105-116.

Schaar, P. (2000): Die Möglichkeiten der Datenschutzaufsichtsbehörden (Possibilities of National Privacy Protection Authorities). In Bäumler, H. (Eds.). *E-Privacy*. Braunschweig, Wiesbaden:Vieweg, 69-76.

Sever, J. et al. (1999). IBM Multi-National Consumer Privacy Survey (Study #: 938568). Accessed September 5, 2000 at http://www.ibm.com/services/files/privacy_survey_oct991.pdf

Shapiro, C., & Varian, H.R. (1999). *Information Rules: A Strategic Guide to the Network Economy*. Boston: Harvard Business School Press.

Smith, R. (2000). Web Bug search page. Accessed September 5, 2000 at http://www.tiac.net/users/smiths/privacy/wbfind.htm

van Gigch, J.P. (2000). Do We Need to Impose More Regulation Upon the World Wide Web? – A Metasystem Analysis. *Informing Science*, 3(3), 109-116.

Vervest, P., & Dunn, A. (2000). *How to Win Customers in the Digital World*. Berlin, Heidelberg: Springer-Verlag.

Wiese, M. (2000). Unfreiwillige Spuren im Netz (Unintentional Tracks in the Net). In: Bäumler, H. (Eds.). *E-Privacy*. Braunschweig, Wiesbaden:Vieweg, 9-19.

Biography

Dirk Frosch-Wilke is a Professor of Business Information Systems at the University of Applied Sciences Kiel. His research interests include the strategic applications of information technology to organizational productivity, electronic commerce and software engineering techniques. He has consulted companies in e-commerce and software development projects.