

For Your Eyes-Only: United States Internet Privacy Laws Play Catch-Up With The European Union Data Directive

Peter L. Banfe, (E-mail: p-banfe@onu.edu), Ohio Northern University
Dexter R. Woods, (E-mail: d-woods@onu.edu), Ohio Northern University

Abstract

Global electronic commerce, driven by the development of the Internet, promises to be a key engine of growth in this century. One of the most contentious issues facing businesses today is the ownership and use of personal data. Europe has taken the lead in this area with a comprehensive approach, the European Union Data Directive, that became effective in 1998. This paper compares the European Union approach to Internet privacy with that of the United States. In comparing the two, the paper includes a brief discussion of current legislation under both approaches and also discusses critical issues in the debate for Internet privacy, including state-directed legislation vs. self-regulation, corporate privacy statements, and the opt-in versus opt-out approaches to consumer protection. The paper offers perspectives on whether the United States will adopt new Internet privacy legislation, and on the feasibility and repercussions of maintaining the current approach.

Introduction

Global electronic commerce promises to be one of the key engines of global economic growth this century. Projected growth rates for business-to-consumer Internet sales between 2001 and 2002 range between 50 and 100% (Jarvis, 2001). Computer ownership and Internet access are both growing at an astounding pace globally. For example, the number of Internet users in China increased from 1,750,000 in July 1998 to 16,900,000 in July 2000, nearly 1000% growth in two years. One of the key issues facing corporations today is the ownership and use of personal data collected on-line during Internet transactions.

One of the major challenges is balancing the need for consumer privacy against the desire to ensure an environment conducive to continued development of e-commerce and the global economy. The European Union has adopted comprehensive social legislation. The United States, however, has relied on corporate self-regulation and a hands-off laissez faire approach. In 1998 a debate raged in the United States regarding Internet consumer privacy, raising the possibility of a more comprehensive legislative approach. Congress introduced over 80 bills, and President Clinton formed a team consisting of Commerce Secretary Daley and Ira Magaziner to warn corporate America to get its privacy house in order or face potentially expensive regulatory action (Joachim, 2001). However, most of the bills languished in committee, and corporations procrastinated in making changes. Accordingly, no comprehensive regulation resulted. After a relative lull, the debate is once again heating up with over three hundred privacy-related bills currently in state legislatures and many others under consideration at the Federal level, including a comprehensive bill introduced in the House of Representatives (Despeignes, 2001; Cantos, Fine, Porcelli, & Selby, 2001).

Readers with comments or questions are encouraged to contact the authors via email.

An understanding of the Internet privacy debate and assistance in navigating the web of current and proposed legislation in the United States and European Union should be of major interest to both academics and practi-

tioners. First, if European firms set the standard for consumer privacy, then commercial sites not conforming to those standards will operate at a disadvantage marketing products and services over the web. Forester Research estimates that the cost of consumer concerns about Internet data privacy amounts to about \$12.4 billion in lost sales annually (Despeignes, 2001). Second, the market for the trade of personal information between the United States and the European Union is estimated at \$120 billion annually (Perine, 2000). US corporations can ill afford to miss out on this potentially lucrative opportunity. Third, it appears that once again, as with quality control standards and ISO 9000, the European Union with its European Union Data Directive has preempted the United States, which now must play catch-up in terms of putting into place the legislative infrastructure to deal with data privacy on the Internet.

The Debate

Prior to the late 1990s consumers in the United States appeared to be generally unconcerned with the issue of online privacy, opting instead to let the free hand of the market guide corporate decisions (Raysman & Brown, 2000). By 1998, however, debate over online privacy intensified because of increased online purchases, Internet fraud, and the enactment of the European Union Data Directive (EUDD) (Grande, 2000). The EUDD's strict protection of consumer privacy set off warning bells in the United States and a flurry of negotiations between the United States and the European Union. The firewall that the EUDD created directly affected US corporations that faced the possibility of being locked out of certain types of Internet transactions with the European Union. EUDD regulations require that EU member nations enact tough laws to ensure the integrity of personal data. The EUDD forbids the transmission of personal data to non-member countries that have not put in place "adequate" safeguards to protect personal data. Unfortunately the term "adequate" is a fairly ambiguous term that has proven difficult to define in negotiations between the United States and Europe.

The EUDD endeavors to "harmonize national laws on processing personal data and protect the rights and freedoms of the persons concerned, in particular their right to privacy." First, EU members can collect personal data only for *specific* and *legitimate* purposes. Second, the consumer must be clearly informed as to the purpose for collection, any third party recipient, whether it is voluntary or required, and the repercussions of refusal to consent to the collection of personal information. Third, the consumer must consent to any collection or use which must be consistent with that consent. Finally, the EUDD mandates the creation of a Working Party on the Protection of Individuals with regard to the Processing of Personal Data, comprised of national and EU-level representatives (European Directive, 1995).

Whereas protection of consumer rights has figured prominently in the EU approach, the US message has been that unfettered e-commerce will benefit everyone by facilitating economic growth. As US Trade Representative Susan G. Esserman stated, "what we're (the United States) seeking to do is prevent barriers (to e-commerce) from being established in the first place" (Burgess, 1999). Unlike the Europeans where privacy has been seen as a fundamental right, in the United States personal data has been to this point viewed as an asset to be bought or sold on the market (Raysman & Brown, 2000). As indicated in the next section, the United States has not passed any comprehensive legislation covering on-line privacy. The United States approach sharply contrasts with the European Union approach. One can characterize the European Union approach as "consumer-oriented social legislation (COSL)" and the United States approach as "growth-oriented self-regulation" (GOSR). Under the US approach, as long as consumers do not complain, and businesses give the impression of having the best interests of the consumer in mind, the tango between government and business continues with minimal regulatory interference. Since the EUDD was enacted in 1998, the US government approach has consisted of two major elements, industry self-regulation and endeavoring to minimize regulatory controls. Commerce Department spokesperson Morrie Goodman voiced the support of the Clinton Administration for this approach when he stated, "We have a long history of voluntary regulation" (Bray, 1999). The new Republican administration is even more resolved to continue this approach.

Naturally, business also supports the idea that the answer lies in self-regulation. Many firms have taken steps to demonstrate their commitment. Both Microsoft and IBM have hired privacy experts to design and manage their privacy functions (Despeignes, 2001). Amex offers "anonymous, secure web-shopping and temporary credit card numbers." DoubleClick now refuses to transact business with customers who do not meet its privacy criteria.

The self-regulation schema currently includes four major components: voluntarily promulgated privacy statements, trust certifications, privacy protection technology, as well as efforts to empower the consumer regarding the use of personal information.

Probably the most crucial element to the self-regulation approach is the voluntary promulgation of privacy statements within the technology industry (Privacy, 2000). Companies have voluntarily adopted privacy statements for three main reasons. First, corporations are sensitive to the risk that inadequate self-regulation could lead to more costly government sponsored regulation. Second, they have done so to quell users' fears that their sensitive personal information would be misused. Third, a recent motivation has been that posting privacy statements clearly and prominently on the website is required if companies are to receive certain types of information from the EU (Privacy, 2000). AOL's online privacy policy is a good example of the types of issues covered in privacy policies. It is seven pages long and covers a number of "dos" and "don'ts" concerning online personal data security, which they refer to as their "eight principles of Privacy". The "eight principles" address the use of personal information, the privacy of consumer online communications, the ability to correct errant information, consumer choice regarding AOL's use of personal data, the safeguarding of data, as well as their intent to keep the consumer informed about changes in that policy (AOL Privacy Policy, 2001).

The authors raise a number of concerns about the effectiveness of current online privacy policies. First, many privacy statements were either drafted by lawyers with an insufficient understanding of technology issues, or by marketing departments with the goal of selling online security to the customer. Second, since many websites link to others, it can become difficult for the consumer to figure out whose privacy statement applies (Ceniceros, 2000). Third, studies have shown that most consumers never take the time to read the statements. Fourth, once the privacy policy has been drafted, procedures normally are not in place to update the policy to be consistent with changes in the corporation's business model or technology. This raises the risk that corporate behavior might evolve to become inconsistent with stated policies. Fifth, many are very skeptical that corporations can be trusted to regulate themselves in a way that ensures consumer welfare (Privacy, 2000).

Detractors also criticize the privacy policy approach from the perspective of risk to the corporation (Privacy, 2000). Privacy policies can create a huge prospective liability for corporations. Clearly delineated privacy policies published on the web are a promise the company must keep or face potential legal repercussions (Grossman, T. & Grossman, 2000; Ceniceros, 2000). A number of recent high profile cases highlight the legal issues raised by published privacy policies, which may never have been raised if those policies had been kept internal to the firm. The most notorious case involves now defunct online toy e-tailer Toysmart. In its online privacy policy the company promised never to share its online customer database. However, during bankruptcy Toysmart announced its intentions to sell that database to the highest bidder (Geocities, 1999). Although a bankruptcy judge rejected a settlement between the Federal Trade Commission (FTC) and Toysmart that would have placed restrictions on that sale, the FTC plans to enter into the fray once again after a buyer has been found. A second landmark case involved DoubleClick, which has been the target of a class action suit. Consumers allege that the company surreptitiously collected private data from unsuspecting Web users. In addition, the online privacy policy stated that the firm would not collect data in a way that allowed for personal identification of data. However, after acquiring Abacus Direct, the firm changed its privacy policy to allow information that it collects to be associated with personally identifiable data. Similarly, Amazon.com/Alexa Internet (a subsidiary of Amazon.com) was sued because its privacy statement implied that data would be used in the aggregate, rather than as personally identifiable data. RealNetworks is being sued both for failing to follow its privacy statement as well as for the method in which it collected consumer information. Plaintiffs claim that the company, via a cookie placed on users' system at registration, covertly tracked music and listening preferences as well as other personal information located on the consumers' hard drives. Then the company allegedly sold the data to a third party. Two other high profile cases involving breaches of online privacy and violations of stated privacy policies include Intuit and Geocities. The Intuit case is of particular note due to the sensitivity of the personal data involved. Plaintiffs allege that Intuit, via its Quicken.com website, collected personal financial data and shared this data with third parties in violation of its own stated privacy policy.

In a number of these high profile cases the FTC and the federal courts appear to be favoring leniency for corporations. For example, GeoCities and the FTC settled their case out of court. The settlement requires that

GeoCities post a clear and prominent policy statement on the web, allowing users' access to remove personal information. Also, GeoCities must now obtain "verifiable" consent from parents prior to collecting personal information from children (Geocities, 1999). Also, early in the year, a federal judge dismissed all private lawsuits against DoubleClick. The FTC did the same, with the agreement that DoubleClick carefully revise its data privacy policies. Amazon has also managed to settle its privacy lawsuits out of court. In September of 2000, Amazon revised its privacy policies to fend off potential litigation. The Wall Street Journal announced in May that the FTC had agreed not to review modifications to Amazon's privacy policy in 2000 as it could not identify any wrongdoing. In what appears to be something of a publicity stunt, Amazon announced that it would pay \$40 to any customer who could prove that the company had improperly gathered personal information, thereby placing the burden of proof onto the consumer (Prior, 2001). On the other hand, because of the risk of costly potential litigation, every firm that does a significant amount of business over the Internet should take steps to seriously address the privacy issue. A first logical step would be to set up a separate privacy function staffed with personnel with training on the issue, working in tandem with corporate legal counsel (Grossman, T. & Grossman, 2000). The privacy staff should be charged with constantly monitoring the consistency of privacy policies with corporate behavior and managing the evolution of those policies with changes in technology and the firm's business model.

Other than voluntary privacy statements, firms have proposed to self-regulate in a number of other ways. One mechanism is to seek a sort of "Good Housekeeping" seal of approval from an independent, non-profit entity, which audits the firm's compliance with its own privacy policies. TRUSTe is probably the most familiar of these entities. If a firm satisfies the entity's criteria by meeting certain minimum standards, then the TRUSTe certification is posted prominently on the website (Privacy, 2000). The Better Business Bureau has launched its own program, and TrustUK, an entity sponsored by the British government and offering similar e-trade trust services, began in July of 2000. Clicksure and Trust-On-Line, to name a few, offer similar services. Whether these entities can be held liable for not identifying inconsistencies between a firm's stated policies and behavior has not yet been litigated.

Another self-regulatory mechanism promoted by the industry is "P3P", Platform for Privacy Preferences, developed by the World Wide Web Consortium, a not-for-profit entity promoting common standards for the Internet. What P3P promises to do is to allow users to pre-screen web sites to determine whether or not it satisfies the consumer's privacy criteria. The latest version of Microsoft's Internet Explorer will contain P3P technology as part of the program. Critics claim that P3P has its own inherent problems. First of all, it does not guarantee that companies will not change their policies after they collect the personal data. A prominent example is Toysmart which, contrary to its privacy policy, decided to sell personal information to the highest bidder during bankruptcy. Second, P3P technology cannot guard against the possibility that as consumers' preferences change, some customers may begin to feel uncomfortable about data they previously consented to being collected.

Besides the P3P technology, companies can empower consumers regarding usage of their personal data by allowing them to either "opt-in" or "opt-out" of the collection of personal data. Opt-in is by far the stricter solution. Companies that grant consumers the right to opt-in cannot use any personal information at all unless the consumer consents to that use. Therefore, with opt-in the data inventory is left empty unless the consumer agrees to items being entered into that inventory. Opt-out on the other hand allows e-businesses to gather and use any personal information that the consumer does not clearly object to being used. Therefore, in opt-out the data inventory will be filled unless the consumer objects, addressing each type of data specifically to be withheld. Senator Hollings introduced an opt-in bill in Congress in 2000, but the bill died in committee with little hope of reintroduction in the near future. Consumers favor the opt-in approach. Recent research by Harris Interactive Inc. indicates that 84% of adults would not permit a website to share personal information with a third party. In addition, 86% would want websites to request permission (opt-in) before using any personal information for marketing purposes, including names, addresses and telephone numbers (Jarvis, 2001). Of course marketers support the opt-out approach. The Clinton administration and the FTC both supported the opt-out approach to personal data privacy (Consumers' Views, 2000). Most bills currently in Congress also favor this approach. Considering the current pro-business Republican administration under Bush, chances are that any bill that becomes law will favor the opt-out approach.

In addition to self-regulation, the United States approach has favored efforts to keep regulatory control of the Internet to a minimum. As regards the EUDD, since 1998 agencies of the United States Government have been

negotiating feverishly to try to satisfy EU demands for “adequate protection” (European Directive, 1995). During these negotiations, the United States side has continually countered the stiff pro-consumer demands inherent to the EUDD with proposals for self-regulation. For example, a joint EU/US statement on electronic commerce in 1997 stated that “unnecessary existing legal and regulatory barriers should be eliminated and the emergence of new ones should be prevented” (Joint Statement, 1997). And as is stated in a December 18, 2000 Statement of the United States and the European Union on Building Consumer Confidence in E-Commerce and the Role of Alternative Dispute Resolution “the means of building consumer confidence and consumer protection in shopping on-line is good business practice and enforceable self-regulatory programs such as codes of conduct and trustmarks” (Statement on Confidence, 2000). More recently, the Bush administration has been resisting EU demands that the US banking industry adhere to the EU’s consumer privacy laws.

Consistent with the US desire to minimize regulatory controls, the United States and the European Union have negotiated a compromise to satisfy demands for “adequate protection” of transferred information. This voluntary “Safe Harbor” scheme became active in April 1999. Entering into a Safe Harbor enables an organization to “receive, transmit, process and use personal data” from the European Union, within the bounds of Safe Harbor principles (European Directive, 1995). The FTC is the primary enforcement agency for the Safe Harbor arrangement. An organization may participate in a Safe Harbor in three ways. First, it can become a member of a privacy organization that adheres to those principles. A second method is via self-certification. Third, it may be an organization already subject to governmental regulation regarding data privacy (Commission Decision 95/46/EC, Annex I, 2000). Safe Harbor principles address a number of important issues. The first issue is “notice”. The consumer must be clearly and conspicuously notified why the data is being collected, the intended use, third party use, and options for the consumer to deny disclosure. Usually this requires that the privacy policy be posted conspicuously on the website. The principles also facilitate consumer choice by allowing them opt-in for sensitive personal information and opt-out for third party transfer of personal data or use other than originally intended. The organization must provide “reasonable” security against misuse, theft, abuse, loss, disclosure, alteration and destruction of personal data. The organization must also take “reasonable” steps to insure the integrity of the data in terms of its accuracy, timeliness, and completeness. Finally, consumers must have a “reasonable” right to access data collected and to correct, amend or delete inaccuracies (Decision 95/46/EC, Annex II, 2000).

Current State of Federal Legislation Concerning Online Privacy

Currently US Internet privacy is covered by a patchwork of federal and state privacy laws, most of which were not crafted to directly deal with the issue, but many of which have taken a prominent place in current litigation. One example is the Electronic Commerce Privacy Act (ECPA), which is a 1986 revision of the federal wiretap statute. The law prohibits both the unauthorized accessing of computer facilities or networks and prohibits exceeding authorization limitations on access. It also prohibits the unauthorized interception of data. The law, which provides for both civil and criminal penalties, has found its way into most Internet privacy litigation. Another law, the Computer Abuse and Fraud Act, also known as the anti-hacking statute, also prohibits unauthorized access to computer facilities or exceeding authorization limitations on access to those facilities. Computers protected under the statute include the broad rubric of those used in interstate commerce or communications. In addition it prohibits the transmitting of a computer virus to a protected computer with malicious intent. Although to invoke this statute damages must total a minimum of \$5000 in one year, these may be aggregated. Hence, the statute features prominently in class action privacy litigation.

The Children's Online Privacy Act of 1998 (COPPA) is unique in that it is one of the few privacy laws written specifically to address the issue of Internet privacy. The law restricts the collection of private information regarding children under the age of 13 during web surfing activities. This information includes, names, physical and virtual addresses, telephone numbers and social security numbers. Web operators are also prohibited from collecting other personally identifiable data about the child or child's parents. Prior to collecting any of the above data, the web operator must obtain "verifiable consent". Under COPPA, no website can condition the participation in web activities (such as games) on the disclosure of personal information by the child.

Two other statutes of note include the Video Privacy Act (enacted in 1988) and the Cable TV Privacy Act

of 1984. Although the Video Privacy Act was created to protect the privacy of consumers with regard to their video rentals and purchases, it potentially may be applicable to the sale of downloaded or streaming video on demand over the Internet. This carries potential liability for e-tailers like Amazon.com, which engage in the "rental, sale, or delivery of prerecorded video cassette tape or similar audio visual materials" (Video Privacy Act, 1988). The Cable TV Privacy Act of 1984 has recently become potentially relevant to Internet privacy because of the ability of cable operators to offer Internet access. The act states that the "cable operator can not collect personally identifiable information without the prior written or electronic consent of the subscriber concerned" (Cable TV Privacy Act, 1984). The act provides a fairly clear and quite strict "opt-in" approach to data collection. It still remains to be seen how this will affect cable operators supplying Internet access, and whether or not they will be precluded from collecting "click stream" data.


Over the last year, momentum toward a legislative solution to the Internet privacy debate has been growing. As referred to earlier in this paper, a Harris study indicates that consumers appear to prefer more stringent controls over the ability of e-firms to collect and use their personal data. The results of a recent Pew Internet & American Life Project are striking in that they indicate that consumers are willing to grant the government surprisingly broad powers to monitor the Internet in its efforts to reduce cybercrime. This includes even some monitoring capability over personal email messages (Joachim, 2001). In addition, 54% indicate that web tracking invades privacy. Finally, a surprising 94% agree that firms should be disciplined if they violate their own privacy policy (Consumers' Views, 2000). Congress is planning to start debate over a number of significant pieces of web privacy legislative proposals that, if they become law, could have an incredible impact on the cost of doing business over the Internet (Teinowitz, 2001; Sinrod, 2001). Proposals include a prohibition against unauthorized "cookies", extending the jurisdiction of the COPPA (for children) to adults, and broadening the regulatory powers of the FTC (The Consumer Online Privacy and Disclosure Act) (Private Eyes, 2001; Despeignes, 2001).

This paper cannot discuss the large number of Internet privacy bills introduced into Congress, but it summarizes below those that are potentially most important. In 2000 the Student Privacy Protection Act stalled in committee, but there is still a good chance that it, or something similar to it, will be reintroduced soon. If it becomes law, the Student Privacy Protection Act would prevent federal funded educational institutions from selling student personal data without express parental consent (Private Eyes, 2001). At least two other proposals would directly affect "spyware" programs that have the ability to access personal information on the hard drives of consumers without their consent. The Social Security Online Privacy Protection Act would regulate the use of social security numbers and related personally identifiable information by interactive computer services. A number of other bills would either regulate or prohibit Spam, or the transmission of unsolicited email advertisements. Finally, the Consumer Online Privacy Act is also currently before Congress. This bill would prohibit the linking of Internet Provider web addresses with personal information, and the tracking of web-surfers' Internet activities.

Probably the most significant piece of legislation is the Consumer Internet Privacy Enhancement Act (CIPEA) introduced in Congress this year by Representatives Anna Eshoo and Chris Cannon. The bill is of the "opt-out" type, and endeavors to "empower the consumers" to protect their privacy on the Internet. The Act is a comprehensive approach that contains a number of provisions of critical importance to e-tailers, many of which are similar to those of the EUDD. Under CIPEA, a clear and conspicuous policy must be posted on the web outlining the following: the identity of the web operator, any third parties who have access to or may purchase the data, the types of data collected, a description of data security measures in place, and a name, physical and email address, and telephone number for the Web operator (Cantos, Fine, Porcelli, & Selby, 2001). Basically CIPEA would prohibit the collection of personally identifiable data unless the Web operator informs the consumer, and allows the consumer to limit the disclosure and use of the information gathered (Young, 2001).

Conclusions

The European Union has taken the initiative on Internet privacy legislation with the comprehensive approach of the EUDD. Similar to the "consumer-oriented social legislation" (COSR) approach of the European Union, in April of 2000, Canada passed the Personal Information Protection and Electronic Documents Act, which became effective January 1, 2001. It requires that firms that collect data online inform customers about what they are

gathering, why they are gathering it, and how it will be used. The Law will take full effect by 2004 (Internet Privacy, 2001; Perine, 2000). Currently, Internet privacy in the United States is governed by a patchwork of state and federal laws. No overarching comprehensive legislation has been passed. The United States is playing catch-up, with a plethora of Internet privacy related bills facing Congress. One of the most significant bills at this point is the Consumer Internet Privacy Enhancement Act that offers a somewhat more comprehensive “opt-out” approach to protecting the privacy of individuals online. The Internet privacy debate has been heating up as of late. Continuing breaches of personal privacy and highly publicized cases of misuse of that information by firms which violate their own privacy policies has sparked consumer ire. Congress appears ready for fairly significant change in the legislative approach. On the other hand, the Bush administration seems to be pulling back, favoring a continuation of the “growth-oriented self-regulation” (GOSR) approach. Clearly, the stage is set for change. However, the question is, how effective will the adherents to GOSR within the current administration be in forestalling any comprehensive legislative agenda? What will emerge from the conflict between the historical preference of the United States political-economic culture for a GOSR-type approach that favors corporate self-regulation versus an increasingly influential European Union COSR-type approach that favors consumers over big business and state directed comprehensive regulation? 

References

1. America Online Privacy Policy (2001), at http://corp.aol.com/privacy_policy.html.
2. Bray, H. (1999, April 21). US, EU agrees on net privacy rules: Europeans would get more protection than Americans. *Boston Globe, Third Edition, Business Section*, p. D1.
3. Burgess, J. (1999, November 7). An E-Common Market puts borders to test as Internet commerce goes global, countries weigh new barriers. *Washington Post, Financial Section*, p. H1.
4. Cable TV Privacy Act (1984). 47 U.S.C. §551.
5. Cantos, L., Fine, L., Porcelli, N., & Selby, S. (2001). House considers opt-out consumer Internet privacy legislation. *Intellectual Property & Technology Law Journal*, 13, (4), 23-24.
6. Cenicerros, R. (2000, May 22). Internet privacy liability growing. *Business Insurance*, 34, p. 1.
7. Commission Decision 95/46/EC (2000, July 26). Annex I, on the adequacy of the protection provided by the safe harbor principles issued by Dept. of Commerce. *Official Journal of the European Communities (L 215) 10*.
8. Commission Decision 95/46/EC (2000, July 26). Annex II, frequently asked questions on the adequacy of the protection provided by the safe harbor principles issued by Dept. of Commerce. *Official Journal of the European Communities (L 215) 13*.
9. Consumers' views split on Internet privacy (2000, August 21). *New York Times, National Edition*, p. C3.
10. Despeignes, P. (February 28, 2001). Exorcising the ghost in the Internet machine: Online security. *Financial Times, London Edition, Inside Track*, p. 14.
11. European Directive on the Protection of Personal Data (1995), Council Directive 95/46/EC, at <http://europa.eu.int/scadplus/leg/en/lvb/114012.html>.
12. Geocities, Docket No. C-3849 (1999, February 12). Final Order, at www.ftc.gov/os/1999/9902/9823015d%26o.html.
13. Grande, C. (October 19, 2000). Crime wave has websites rushing to fill the breach: Industry leaders find it far from simple to co-ordinate a global approach to better Internet security. *Financial Times, London Edition, International Economy*, p. 14.
14. Grossman, T. & Grossman, A (2000, September 12), Lifting the veil on Internet privacy. *Mealey's Cyber-Tech Litigation*, 2 (7).
15. Internet privacy law now on-line (2001, January 2). *Globe & Mail*, p. B4.
16. Jarvis, S. (2001, April 23). Maybe this year. *Marketing News*, 35_(9), 1, 13-14.
17. Joachim, D. (2001, April 16). Internet privacy debate is dead. *Internetweek*, 857, 20.
18. Joint E.U.-U.S. statement on electronic commerce (1997, December 5), at <http://www.qlinks.net/comdocs/eu-us.html>.
19. Perine, K., (2000, June 26). Net privacy proposal in jeopardy. *The Standard*, p. 7, at <http://www.thestandard.com/article/display/0,1151,16387,00.html>.
20. Prior, M. (2001, May 21). New view of data assets alters on-line privacy policies. *DSN Retailing Today*,

- 40 (10), 6.
21. Privacy: Don't ask technology to do the job (2000, June 26). *Business Week*.
 22. Private eyes (2001, April 16), *Insight on the News*, 17 (14), 26.
 23. Raysman, R. & Brown, P. (2000, October 10). International privacy: Safe harbor protection for personal data. *New York Law Journal, Computer Law Section*, p. 3.
 24. Sinrod, E. (2001, February 19). Demanding privacy. *Computerworld*, 35, (8), 36.
 25. Statement of the United States and the European Union on building consumer confidence in e-commerce and the role of alternative dispute resolution (2000, December 18), at http://www.ecommerce.gov/joint_statements/EU_ADR1-5-01.html.
 26. Teinowitz, I. (2001, March 12). House Means to act on Web issues. *Advertising Age*, 72 (11), 42.
 27. Video Privacy Act (1988). 18 U.S.C. §2710.
 28. Vogt, S. (2000, September 11). Online privacy laws all over the map. *Strategy, Perspectives, The Legal File*, p. 12.
 29. Young, D. (2001, April 1). Privacy vs. data collection. *Wireless Review*, 18 (7), 10.