Public Comment on Barriers to Electronic Commerce
U.S. Department of Commerce -- Office of the General Counsel; Laws or Regulations Posing Barriers to Electronic Commerce

Submitted March 17, 2000

Sarah Andrews
Policy Analyst
andrews@epic.org

Andrew Shen
Policy Analyst
shen@epic.org

Electronic Privacy Information Center (EPIC)
http://www.epic.org
Tel: (202) 544-9240
Fax: (202) 547-5482

Pursuant to the notice published by the United States Department of Commerce, Office of the General Counsel on February 1, 2000, the Electronic Privacy Information Center (EPIC), formally submits the following comments.

EPIC is a public interest research center located in Washington, D.C. that has extensive expertise in privacy and cryptography, both domestically and internationally.

EPIC is also a member of the Trans Atlantic Consumer Dialogue, a coalition of over 60 American and European consumer groups.

LEGAL BARRIERS TO ELECTRONIC COMMERCE

EXECUTIVE SUMMARY

For electronic commerce to reach its full potential, the United States has a vital role to ensure that online consumers will feel comfortable conducting business. To that end, the U.S. will in some cases have to support new legal protections and in other cases to remove existing burdensome regulations.

In order to create a favorable legal environment for the growth of the Internet, the United States should develop a strong federal standard for online privacy protection. The development and dissemination of cryptography -- necessary for secure online communication -- should be widely encouraged. In addition, the U.S. has a unique opportunity to establish high international consumer protection standards that offer simple, predictable rules for companies and individuals.

The Organization for Economic Cooperation and Development's (OECD) guidelines for privacy protection, cryptography policy, and consumer protection in electronic commerce provide useful frameworks for the development of U.S. policy that will promote consumer confidence and reduce barriers to electronic commerce.[1]

PRIVACY PROTECTION

Consumers are unsatisfied by the current level of consumer privacy protection and support a strong legally enforceable standard.

American consumers currently have high levels of concern about online privacy and a corresponding reluctance to shop online. EPIC has found that such reluctance is justified. In "Surfer Beware 3: Privacy Policies without Privacy Protection", EPIC documented that none of the top 100 shopping sites provided necessary elements of privacy protection in their privacy policies.[2] Earlier surveys found companies similarly slow to respond to consumer privacy concerns. In 1997, EPIC found that only 17 out of the 100 most popular sites had privacy policies and that none provided adequate protection.[3] In 1998, EPIC surveyed the practices of members of the Direct Marketing Association (DMA) -- a

---

[1] These guidelines are available through the OECD's Directorate of Science, Technology, and Industry at http://www.oecd.org/dsti/sti/

[2] "Surfer Beware 3: Privacy Policies without Privacy Protection" is available at http://www.epic.org/reports/surfer-beware3.html

[3] "Surfer Beware: Personal Privacy and the Internet" is available at http://www.epic.org/reports/surfer-beware.html

self-regulatory organization -- and found that of the forty companies that had websites, only three of them had privacy policies that complied with the DMA's own guidelines.[4]

The lack of consumer trust in the Internet is significant. Industry newsletter Privacy & American Business found that 61% of U.S. Internet users have at some time refused to purchase a product online because of privacy concerns.[5] E-commerce industry analysts at Forrester Research have noted that privacy is consistently the number one concern of online consumers and estimate that in 1999 these concerns resulted in $2.8 billion in lost sales.[6] To put this amount into perspective, the 1999 holiday shopping season was declared a success upon reaching $7 billion in total sales.[7]

Public support for legally enforceable privacy protection is clear. In a poll recently released by Business Week, Harris Interactive found that 57% of those polled think that "the government should pass laws now for how personal information can be collected and used on the Internet" and that only 15% supported letting "groups develop voluntary privacy standards, but not take action until real problems arise."[8]

Government officials close to the recent privacy controversies have also found the current state of privacy protection lacking. Robert Pitofsky, Chairman of the Federal Trade Commission, recently stated, "Given the invasions of privacy that we have seen in the early stages of development of online commerce -- some involving the illegal collection of personal information from kids -- and the constant concern by online participants about invasions of their privacy, the do-nothing option does not seem appealing."[9]

The absence of legal enforceable privacy protection threatens the expansion of American electronic commerce into foreign markets.

The European Union has adopted comprehensive and enforceable guidelines for privacy protection online and offline that appropriately protects the privacy interests of consumers. Since the passage of the EU Data Protection Directive, the U.S. had been in negotiations over a Safe Harbor -- essentially what needs to be added to the current U.S.

---

[4] "Surfer Beware 2: Notice is Not Enough" is available at http://www.epic.org/reports/surfer-beware.html

[5] "The IBM-Harris Multi-National Consumer Privacy Survey," Privacy & American Business, January 2000, 11.

[6] "Trails of personal info compromise Net shoppers' privacy," USA Today, December 20, 1999, 3B.

[7] "Online Holiday Sales Hit $7 Billion, Consumer Satisfaction Rising," Jupiter Communications Press Release, January 13, 2000.

[8] "Online Privacy: It's Time for Rules in Wonderland," Business Week, March 20, 2000, 96.

[9] "Electronic Commerce and Beyond: Challenges of the New Digital Age," Remarks by Robert Pitofsky, Chairman, Federal Trade Commission, The Woodrow Wilson Center: Sovereignty in the Digital Age Series, February 10, 2000. Available at http://www.ftc.gov/speeches/pitofsky/rpwilson2.htm

system -- that would satisfy the adequacy requirement. Negotiations have continued for two and a half years and no agreement has yet been reached. Without such an agreement, the ability of U.S. companies to serve European customers is in doubt.

The passage of the European Union Data Protection Directive and the lack of a comparable law in the United States threaten to curtail a valuable market. A study by the Boston Consulting Group (BCG) estimated that online European retail sales reached $3.6 billion in 1999.[10] Other trading partners such as Canada are also in the process of passing comprehensive privacy legislation that would include provisions for blocking data flow to countries that do not offer adequate protection.

The OECD Privacy Guidelines are the proper model for U.S. online privacy protection.

The OECD Guidelines offer a robust system of privacy protection that apply to any sector and to any technology. They only dictate what information should be collected and how it can be used -- but they do not specify how a company should implement these privacy protections. Due to the neutral way in which the guidelines discuss specifics, it has stood the test of time. The Organization for Economic Cooperation and Development's 1980 Privacy Guidelines were developed more than a full decade before the existence of the World Wide Web yet have been reaffirmed in the 1999 Consumer Protection Guidelines for Electronic Commerce.

CRYPTOGRAPHY

Freely available strong cryptography is necessary to ensure the security of online communications.

A vital factor in the success of electronic commerce will be the free use and availability of strong cryptographic products. Cryptography is used to conceal or verify the contents of electronic documents and to protect files from unauthorized access, alteration and theft. It is a critical, and presently the only reliable, way of safeguarding the security of electronic information. Cryptography can help citizens and businesses defend themselves against fraud, electronic vandalism and the improper disclosure of confidential information. Businesspeople rely on encryption to safeguard sensitive business materials, such as client records, professional communications or trade secrets. Consumers depend on encryption to secure their personal and credit card details against theft or misuse when transacting in the on-line world. If people cannot depend on the confidentiality and authenticity of electronic information, they may revert to more traditional methods of communication and effecting business transactions. As such, the full potential of electronic commerce may never be exploited.

[10] "First America, then the world," The Economist, February 26, 2000, 49.

Attempts by law enforcement to limit the use and dissemination of cryptography will adversely impact electronic commerce.

Due to the possibility of criminal use of encryption products, law enforcement agencies have called for restrictions on unbreakable encryption. The U.S. has traditionally been the leader in these calls for restrictions among the Western world. The most recent initiative in this regard is the Cyberspace Electronic Security Act of 1999 (CESA) [11], which was drafted by Department of Justice officials and transmitted to Congress on September 16, 1999. The expanded powers that the bill gives to law enforcement agencies discourage the public's use of cryptographic products. The powers which would be laid down in CESA for police seizure of keys are questionable as contrary to the Fourth Amendment. Instead of mandating 'probable cause' and contemporaneous notice for the issue of a search warrant in accordance with the Constitutional requirement, CESA bases issue of a search warrant upon obscure requirements such as a finding that there is '*no constitutionally protected expectation of privacy in such plaintext.'* Notice must only be given within 90 days of the disclosure and there is even provision for the indefinite postponement of notice 'on the government's ex parte showing of good cause'.

Restrictions on the export of encryption products also exist and continue to stifle the free use and availability of cryptography. The current export rules place a maze of intricate and administrative requirements in the way of the free export of encryption and in doing so, inadvertently serve as domestic use restrictions. As software companies are slow to produce different versions of the same product, one for domestic use and one for export, imposing strict export controls leaves U.S. citizens with access only to unacceptably weak encryption products.

Strong encryption should be routinely available for all electronic communications and not simply electronic commerce.

Although encryption is widely available to consumer when they engage in electronic transactions, there is still little use of encryption by consumers for routine communications. Export controls and proposals such as CESA continue to discourage the use of encryption by individuals who send e-mail messages, business documents and other private or proprietary information. These controls need to be dropped and companies encouraged to provide the public with greater access to programs that would automatically encrypt all messages and files sent over the Internet.

The OECD Guidelines are the proper model for U.S. cryptography policy.

In implementing a policy on cryptography, the U.S. should take account of the OECD Guidelines for Cryptographic Policy which were published in 1997. These Guidelines set out a generous framework for encryption policies and stress the importance of the availability and choice of strong encryption products. Most importantly, principle 5 of these Guidelines sets out that the fundamental right to privacy should be respected in any

[11] Available at http://www.epic.org/crypto/legislation/cesa/bill_text.html

national cryptography policy. By disregarding traditional principles governing police searches, seizures, and surveillance, the law enforcement powers proposed by CESA are contrary to the OECD Guidelines and must, therefore, be abandoned.

CONSUMER PROTECTION

Consumer protections existing in the off-line world should be applied to electronic transactions.

The growth and profitability of electronic commerce will be drastically reduced if consumer protection is not adequately provided. Unless consumers are satisfied that traditional safeguards which protect their rights in the off-line world will be translated in the 21st century they may not be willing to take full advantage of electronic commerce. If people feel that they are offered less protection and are vulnerable to more abuses in the on line environment they may be willing to sacrifice the advantages and ease of on-line shopping for the security of the brick and mortar world.

As electronic commerce is essentially a global phenomenon, international organizations have an interest in harmonizing the development of national policies. In this key area, international co-operation which focuses on strong technology, neutral and flexible principles backed by secure and effective enforcement is the only way of propelling e-commerce forward and safeguarding vital rights of individuals.

Many consumer groups support the development of international consumer protection standards. For example, the Trans Atlantic Consumer Dialogue presents the following in their statement, "Consumer Protection in Electronic Commerce":

> The EU and the U.S. should support the establishment of minimum standards in e-commerce, including the simplification of contracts, means for cancellation, effective complaint mechanisms, limits on consumer liability, non-enforceability of unreasonable contract provisions, recourse at least to the laws and courts of their home country, and cooperation among governments in support of legal redress. Such minimal standards should provide a functional equivalence to current safeguards offering at least the same levels of protection that would be afforded in the off-line world.[12]

Support of the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce

Regulation of this area in the U.S. should be governed by the recent OCED Guidelines on Consumer Protection which were released in 1999. These Guidelines are predicated on the basis that consumers should not be offered any less protection when participating in

[12] Available at http://www.tacd.org/papers/ecommerce/Ecom-3-99.rtf

electronic commerce than they are in other forms of commerce. The main protections which the Guidelines propose include;

- Fair Business, Advertising and Marketing Practices
- Sufficient disclosure of relevant information
- A clear and unambiguous confirmation process
- Proper means of redress in the case of cross border disputes and clarification of applicable jurisdiction.
- A secure method of payment, minimizing the risk of financial loss.
- A reliable system of international Alternative Dispute Resolution to provide a workable alternative to litigation, which may be costly and disproportionate in the case of long distance transactions

As a signatory to the OECD, the U.S. needs to implement these principles into domestic law. Only then will the current standards of protection that exist for consumers in the off-line world be guaranteed in electronic commerce.

These three areas of concern need to be addressed by the U.S. in order to promote trust and confidence in electronic commerce and remove any barriers to its full development. In doing so, the U.S. should be influenced by the sound principles set out in the OECD Guidelines. We believe that the U.S. needs not only to embrace these principles but continue its co-operation with its international partners to ensure their effective implementation in national and international law.